

A kriptovaluták megjelenése, elterjedése és a jelenséggel szemben lehetséges jogi válaszlépések

JÁMBOR Gellért¹

A pénz – mint hivatalos csereeszköz – egyik legfontosabb jellemzője, hogy az állam saját hatáskörébe vonja annak kibocsátását, a kibocsátás mennyiségének meghatározásán keresztül pedig az értékének meghatározását is.² A pénzkibocsátás jogát Magyarországon az állam a Magyar Nemzeti Bankon keresztül gyakorolja.³ A kriptovaluták ezzel szemben a pénz fejlődésének korai fázisára emlékeztetnek, szabad csereeszközként funkcionálnak valamely polgári jogilag értékelhető ügyletben. Az államnak nincsen ráhatása sem a kibocsátásukra, sem a bevonásukra, miként arra sem, hogy azok értékét a mennyiség meghatározásán keresztül inflálja vagy éppen deflálja. Fontos megjegyezni, hogy a kriptovaluták pénzforgalmi szabályozás alóli kivettsége sokszor azt eredményezi, hogy olyan tiltott jogügyleteknél szolgálhatnak csereértékként, amelyeket egyébként a jog tiltana, így például terrorizmus finanszírozása, kábítószer vagy más tiltott anyagok forgalmazása. A kriptovaluta magában foglalja az összes digitálisan létrehozott pénzeszközt, amely kriptográfiai titkosítás, „hashelés” útján jött létre. A hashelés pedig olyan digitális folyamat, amely képes visszafordíthatatlan matematikai művelet segítségével egy tetszőleges adatfolyamatot a megadott méretre tömöríteni.⁴ A tanulmány célja annak bemutatása, hogy a kriptovaluták milyen kihívást jelentenek a jogalkalmazók számára amiatt, hogy nem állnak pénzforgalmi szabályozás alatt, s az újfajta jelenséggel szemben milyen jellegű jogi szabályozás lehetséges, illetve mely jogterületeken lenne szükséges további jogalkotási folyamat megvalósítása.

Kulcsszavak: kriptovaluták, titkosítás, blokkláncelmélet, lefoglalás

A kriptovalutákról általában

A kriptovaluták létrejötte szorosan kapcsolódik a bizalom kérdéséhez. Az alapjául szolgáló blokklánc- (*blockchain*-) technológia 2008 novemberében kapott nagyobb figyelmet, amikor valaki(k) Satoshi Nakamoto álnév alatt javaslatot tett(ek) közzé a Cryptography levelezőlistán, amely forradalmian új megoldást mutatott

¹ Bírósági titkár, Tapolcai Járásbíróság; PhD, ELTE Állam- és Jogiudományi Kar Doktori Iskola, e-mail: JamborG@birosag.hu

² HEGEDŰS-LÉNÁRD – ÚDVARY 2021: 9.

³ POLT 2021: 421.

⁴ HEGEDŰS-LÉNÁRD – ÚDVARY 2021: 9.

be a központi elszámoló felek által működtetett fizetési rendszerekhez képest. Korábban a digitális tranzakció csak úgy volt lehetséges, hogy arról duplikátum keletkezett, amelyet a felek egy mindkettőjük által megbízhatónak tartott harmadik félre (a pénzügyi intézet) bíztak. Azonban a 2008-as nagy pénzügyi válság, a bankokba és pénzügyi közvetítőkhöz vetett bizalom hiánya elvezetett oda, hogy felmerüljön az igény a közvetítő nélküli tranzakciókra. A cél egy olyan rendszer kialakítása volt, amely alapvetően bizalommentes, kizárólag a kapcsolódó matematikai számítások jelentik az alapját. Satoshi Nakamoto már említett kilencoldalas javaslata a Bitcoin nevet kapta. Ez volt minden idők legelső kriptográfiai alapokon nyugvó, decentralizált és bizalommentes fizetési technológiai koncepciója, amelynek legfőbb célja a valós idejű fizetések lebonyolítására való képesség mellett a központi harmadik féltől – aki nyomon követi, teljesíti, elszámolja a pénzforgalmat, valamint számlát vezet a szereplőknek – független, megosztott nyilvántartási könyv létrehozása volt. Ebben a fő problémát az a kihívás jelentette, hogy meg kellett találni a módot arra, hogy egy adott pénzegység csak egyszer legyen elkölthető, vagyis kizárható legyen a hamisítás lehetősége. Ezt Satoshi úgy kívánta áthidalni, hogy egyenlő felek közötti *peer-to-peer* (azaz egymással közvetlenül kommunikáló számítógépek segítségével), mindenki számára nyitott és elérhető hálózaton zajlanak a tranzakciók és azok hitelesítése. A tranzakciót elindító a teljes közösség előtt bejelenti tranzakciós szándékát, illetve a lényeges információkat a tranzakcióval kapcsolatosan, és egy egyedi azonosítóval is ellátja azt. A hálózat többi résztvevője pedig hitelesíti ezt a bejelentett tranzakciót. Az igazán forradalmi megoldás azonban az, hogy a tranzakciók hitelesítését szabadpiaci alapokra helyezve érdekeltté teszi benne a hálózaton lévőköt, sőt versenyezteti is őket. Ennek módja az, hogy a hitelesítéshez használt véletlenszerűen generált hashkódok nagy erőforrásigényes visszafejtésének elvégzése után az abban részt vevők jutalomban részesülnek. Ez a jutalom a bitcoin, míg a hitelesítésben részt vevők a történelmi aranyásók mintájára a bányászok. Maga a folyamat ma kriptovaluta-bányászatként lehet ismert sokak számára. Ezáltal nemcsak kizárható a központi fél az egész rendszerből, de a verseny biztosítja azt, hogy az így keletkezett rendszer működőképes és fenntartható legyen, valamint elejét vegye a visszaéléseknek. A Satoshi Nakamoto által megálmodott hitelesítési rendszer lett a blokklánc, az összes kriptovaluta alapja. A blokklánc nem más, mint egy megosztott nyilvántartási könyv, tranzakciókat tartalmazó, decentralizált adatbázis, amelyet nem központilag, hanem számos rendszerben vezetnek és tartanak nyilván. A blokkokra tagolt adatokat saját egyedi azonosítóval is ellátják, amely egy időbélyegből és digitális aláírásból áll. Ezeket a blokkokat kriptográfiai eljárással egymásra fűzik, ahogy újabb és újabb tranzakciókra kerül sor, ezt pedig a rendszer többi résztvevője hitelesíti. Ezek utólag megmásíthatatlanok és visszavonhatatlanok, így garantálják a fizetési rendszer integritását. A harmadik, központi fél hiánya gyors és kis költséggel járó átutalásokat tesz lehetővé. A blokkláncok megváltoztathatatlansága biztosítja az elosztott bizalmat is, mivel szinte lehetetlen megváltoztatni

a blokkláncokban tárolt tranzakciókat, és az összes korábbi tranzakció ellenőrizhető és nyomon követhető.⁵

A kriptovaluták fajtái, jellemzői

A legelső és azóta is töretlen népszerűségnek örvendő Bitcoin mellett léteznek egyéb kriptopénzek is, ezeket összefoglalóan *altcoinoknak* nevezik. Ezekből 2020-ra már több mint ötezer létezett, és mind valamilyen egyedi konstrukciót kínál az érdeklődők számára. Ezeknél két különböző típus különböztethető meg: azok az érmék, amelyek a Bitcoin eredeti, nyílt forráskódú protokollját használják (például a Litecoin) és azon érmék, amelyek a Bitcointól eltérő protokollal működnek (például az Ethereum). Az altcoinok közé sorolható a blokklánc-technológia másik nagy úttörője, az Ethereum, amely a hitelesítésben részt vevő bányászok számára ether nevű kriptovalutát juttat. Ez a rendszer annyiban másabb, mint a Bitcoin és az annak mintájára megjelent egyéb kriptopénzek, hogy ez más decentralizált eszközök (az úgynevezett „okosszerződések”) számára teremt működési felületet. Fontos itt még megemlíteni a Monero nevű altcoint is, amely elsősorban a titkosítást helyezi előtérbe. Ennek érdekében érméi teljes egészében helyettesíthetők egymással, ami azt jelenti, hogy szemben a Bitcoinnal, nem lehet bizonyos érmeiket feketelistára tenni a hozzájuk kötődő korábbi illegális tranzakciók miatt, amelyeket ezeknél az érmeknél a blokklánc örökre megőriz.⁶

Összefoglalva elmondható, hogy a Bitcoin volt az első kriptovaluta, ez az alapja az összes többi kriptovalutának. A kriptovaluták pénzügyi felügyeleti rendszer előli menekülést hivatottak szolgálni, ugyanis titkosítási eljárásokat használnak. A tranzakciók anonimak, olyan főkönyvet használnak, ahol nincs központi szerver, hanem ez a főkönyv egy bizonyos számítógépen van rajta, egy bányászgépen, amely egy nagy teljesítményű számítógép.⁷ Az anonimitás – vagy sok esetben inkább csak pszeudonimitás – a kriptovaluták egyik legfontosabb jellemzője, elvégre az érme nem névre szól, egy személy se kapcsolható közvetlenül valamely tárcához vagy tranzakcióhoz. Csak az dönti el a kriptovaluta használhatóságát, hogy ki van az ehhez szükséges titkosítási kulcs birtokában, miközben egyúttal az utolsó azzal végzett tranzakció címzettjeként jegyezték be az adott érmehez tartozó blokkláncban. Az anonimitás foka az egyes kriptovalutáknál jelentősen eltérhet. A korábban már említett Monero esetén például az összes tranzakció teljesen rejtve van a kriptográfia mögött, ami egyaránt titkosítja a feladó és címzett feleket, valamint az átutalt összegeket. Ezzel szemben a Bitcoinnál a főkönyv szabadon nézgethető, elemezhető, az egyes érmékhez tartozó blokklánc annak kibányászásáig visszakövethető. Ugyan a Bitcoin esetén az egyes

⁵ DORNFELD 2021: 211–213.

⁶ DORNFELD 2021: 213.

⁷ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17-e között megtartott online konferencián elhangzó szakmai előadás.

érmék felhasználói alapvetően teljesen ismeretlenek, azonban a címek közötti utalások iránya, azok ideje és nagysága mindenki számára látható. Ez azt jelenti, hogy ha a láncolatban sikerül valakit azonosítani, akkor onnantól kezdve a teljes utalás története visszakövethetővé válik.⁸

A bitcoin tehát a blokklánc révén működtethető, továbbá azt is meghatározták, hogy összesen 21 millió lehet belőle forgalomban. Kérdés, hogyan lehet hozzájutni a bitcoinhoz:

- bányászat útján (szükséges hozzá egy úgynevezett „bányászszoftver”);
- utalás révén más felhasználótól;
- bitcoin-automatából is lehet vásárolni;
- készpénzért cserébe a felhasználó kap megfelelő bitcoint;
- hozzá lehet jutni a bitcoinhoz ezenkívül még csere és csalás révén is.

Egy tranzakció nagyjából 10 percet igényel. A rendszerben az is szabályozott, hogyan változtathatók meg a szabályok. Összesen 50%+1 többség szükséges a szabályok megváltoztatásához. A bitcoin gyenge pontja a volatilitása, az árfolyam-ingadozás magas, valójában nincs semmilyen mögöttes értéke. A bitcoin küldéséhez és fogadásához kulcsokra van szükség (nyilvános kulcsra és privátkulcsra). Lényegében a bitcoin átadható a felhasználók között, mint az arany.⁹

A második legnagyobb virtuális fizetőeszköz az Ethereum, amely a blokklánc-technológia másik nagy úttörője, saját programmal, „okosszerződés” eszközzel, feltételrendszerrel rendelkezik, ennek mentén teremt működési felületet. Az okosszerződések (*smart contracts*) alkalmazását először az 1990-es években Nick Szabo vetette fel. Szabo szerint az okosszerződés nem azt jelenti, hogy mesterséges intelligenciát alkalmaznak, csak azt, hogy a számítógépes programban tárolt szerződési feltételeket automatikusan végrehajtják, ha azoknak az előfeltételei megvalósulnak. Ennek a gyakorlati megoldása lett, hogy a tranzakciót blokkláncokban tárolják, replikálják és frissítik, a szerződést pedig automatikusan végrehajtják.¹⁰

A harmadik nagyobb kriptovaluta a Tether, amely centralizált, a Tether Company bocsátja ki. Ez a kriptovaluta visszaváltható dollárra, amelyet a kriptotérben végeznek el. Ez a kriptovaluta a dollár virtuális alternatívája, amely magában hordozza a pénzmosás lehetőségét.¹¹

A fent említett három kriptovaluta a digitális pénzeszközök és azon belül is a virtuális pénzek kategóriájába tartozik. A fent bemutatott kriptovalutáknak a következő közös elemei vannak:

Valamilyen érték digitális megjelenése, ami a) a kormány által kibocsátott törvényes fizetőeszköz peer-to-peer (P2P) alternatívájaként hivatott megjelenni, b) álta-

⁸ DORNFELD 2021: 219.

⁹ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

¹⁰ DORNFELD 2021: 213–214.

¹¹ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

lános célú csereeszközként használják (függetlenül bármilyen központi banktól), c) a kriptográfia néven ismert mechanizmus biztosítja működését, valamint d) törvényes fizetőeszközzé váltható és fordítva.¹²

Büntető eljárásjogi, kriminalisztikai válaszleépések

A kriptovaluták büntetőeljárásban való felkutatása és lefoglalása szempontjából csak a bitcoin technológiát mutatom be, tekintettel arra, hogy ez a legrégebben használt és legnépszerűbb virtuális fizetőeszköz.

Felmerülhet a kérdés, hogy mégis milyen módon tudja valaki a kriptovalutáját pénzre váltani és vice versa. Alapvetően – hasonlóan a hagyományos devizaváltásokhoz – magánszemélynél kialakult árfolyamon, erre irányuló tevékenységet végző gazdasági társaságnál meghatározott árfolyamon, illetve virtuális fizetőeszközzel foglalkozó tőzsdéken a keresleti és kínálati viszonyok függvényében kialakult keresztárfolyamon lehet bitcoint váltani. A folyamat egyszerű, a bitcoin eladója a saját pénztárcájából a vevő pénztárcájába utalja a kriptovalutát, a vevő pedig pénzt utal, vagy ad át ellenértékként. A bitcoinváltással foglalkozó gazdasági társaságok, valamint a virtuális fizetőeszköz-tőzsdék általában egy weboldalon keresztül működtetik szolgáltatásaikat. Ezek a cégek a gyakorlati tapasztalatok alapján a tranzakciókat megelőzően általában megkövetelnek ügyfél-azonosítást, amely során a felhasználó személyazonosító okmányainak másolatait szerzik meg. Mindemellett más, az ügyfélhez köthető adatok is jó eséllyel rendelkezésre fognak állni, így a weboldal elérésekor használt IP-cím, mobiltelefonszám, e-mail-cím. Ezen adatok birtokában lépések tehetők a felhasználó beazonosítása érdekében. Megemlítendő még az úgynevezett bitcoin-ATM-ek, amelyek szintén bitcoinváltásra alkalmas készülékek. Ezek az eszközök készpénz kiadására és esetenként annak befogadására is alkalmasak. Készpénz kiadása esetén a felhasználó a saját bitcoinpénztárcájáról a cég bitcoinpénztárcájára utalja a felvenni kívánt deviza bitcoinban kifejezett ellenértékét, valamint megadja a mobiltelefonszámát (nagyobb összegek esetén a vállalkozások fokozottabb ügyfél-azonosítást végeznek), ahová a bitcoin megérkezésekor SMS-ben egy kódot kap, amelyet az ATM-ben megadva a készpénzt magához veheti. A készülékek gyakran képrögzítő berendezéssel felszereltek, amelyek felvételi szintén beszerezhetők az üzemeltetőtől.

A fentiek alkalmazásával arra a kérdésre kaphatunk választ, hogy a célszemélyünk bitcoinnal rendelkezik-e, illetve milyen címet használ, ezután a blokklánc elemzésével több kapcsolódó – lehetőség szerint a pénztárcához tartozó – cím is beazonosítható. Amennyiben a fentiekben felsorolt források egyike sem lelhető fel, vagy olyan állam joghatósága alatt áll, ahol a jogrendszerből eredő eltérések, a nemzetközi jogsegélyre vonatkozó egyezmény hiánya vagy az üzemeltetők együttműkö-

¹² DORNFEELD 2021: 217.

dési szándékának elmaradása miatt nem várható válasz, úgy átvásárlás alkalmazása válhat indokolttá, amely során a hatóság bitcoinot vásárol – azaz vált át – a célszemélytől, aki a kriptovalutát a hatóság által kezelt pénztárcába utalja. Ezáltal az érintett legalább egy címe ismertté válik. Ideális helyzetben – például gyakori bitcoin-váltás esetén – a célszemély több címe is beazonosítható lesz, ami a pénztárcájához tartozó további címek pontosabb felderíthetőségét segíti elő. Magyarországon a legnagyobb virtuálisfizetőeszköz-váltók a CoinCash Ltd., illetve a MrCoin.eu tulajdonosa a Shinrai Kft. Rajtuk kívül számos nagyobb európai váltó működik, mint a Bitstamp vagy a Cex.io, de nemzetközileg ismert tőzsdékkel is találkozhatunk, több ezer ilyen működik világszerte (mint a Coinbase, Bitfinex, Liquid).¹³

A bitcointechnológia lényege a digitális aláírások láncolatában ragadható meg. A bitcoin küldésére és fogadására alkalmas címeket kell generálni, amelyet a program felhasználói kérésre automatikusan létrehoz. Mindegyik bitcoincím két részből áll, egy „nyilvános kulcsból” és egy „privát kulcsból”. A nyilvános kulcs látható, s ezt kell megadniuk a felhasználóknak egymás részére, az utalások kivitelezéséhez. A privát kulccsal pedig – amely viszont rejtve marad a másik fél előtt – a szoftver aláírja a kérdéses tranzakciót. A nyilvános kulcsokat és a hozzájuk tartozó privát kulcspárokat a wallet.dat nevű fájlban tárolja a program a számítógép merevlemezén. A bitcoinhálózat a rajta keresztül létrejövő tranzakciókat az egész hálózaton szétküldi, így azok teljesen nyilvánosak.¹⁴

Az átutaláshoz mindenképp szüksége van a felhasználónak egy privát kulcsra, amely P2P alapú, azaz egymással közvetlenül kommunikáló számítógépek segítségével, mindenki számára nyitott és elérhető hálózaton zajlanak a tranzakciók és azok hitelesítése, továbbá egyenleg is lekérhető. A résztvevők maguk hitelesítik a tranzakciókat. Így nincs olyan központi szerv, amelyhez fordulni lehetne adatigénylés vagy lefoglalás érdekében. A tranzakciók a blokkláncban történnek, amelyek 10 perc alatt mennek végbe. Legfeljebb 1 megabájt adatforgalom lehetséges naponta és maximum háromezer tranzakció. A tranzakciókat tartalmazó blokkokban látszik a küldő és fogadó cím és az időbélyegző. A bitcoin előállításához bányászokra van szükség, továbbá nagy teljesítményű bányászgépre, valamint bitcoinok ilyen módú előállításához alkalmas szoftverre. Az előállítás nagyjából 10 percet vesz igénybe, amelyhez bonyolult matematikai számításokat kell végezni. A kriptovaluta magában foglalja az összes digitálisan létrehozott pénzeszközt, amely kriptográfiai titkosítás – más néven „hashelés” (egy digitális folyamat, amely képes visszafordíthatatlan matematikai művelet segítségével egy tetszőleges adatfolyamot egy megadott méretre tömöríteni) – útján jött létre. A bitcoin a kriptovaluták atyja, az első digitális csereeszköz, amelyet a „hashelés” módszerével állítottak elő. Ez az első decentralizált, tisztán peer-to peer alapú digitális pénz, amely lehetővé teszi az online kifizetések küldését és fogadását az érintett felek között. A hashérték megváltoztatása egyoldalú titko-

¹³ TÓTH et al. 2022: 100–101.

¹⁴ HEGEDŰS-LÉNÁRD – UDVARY 2021: 11–12.

sítással történhet, amelyhez a hashértéket be kell mutatni, amelyen szerepel egy digitális pecsét, amely információként szolgálhat az előállításához használt eszköz lefoglalásához. Fontos azt is megemlíteni, hogy egy-egy ilyen bányászgép nagyon sok energiát fogyaszt, ez megjelenhet az áramszámlában, ami szintén áruklódó jel lehet a nyomozók számára. A bányász célja, hogy ő maga hozza létre a következő blokkot, mert akkor jutalmat kap érte. A nyereséghez 4 db 0 számjegyet kell előállítani, amelyhez szintén bonyolult számítás alapján lehet eljutni. A bitcoinérméket kezelő szoftver, a bitcointárca virtuális pénztárcaként funkcionál az egyes felhasználók számítógépén, olyan fájl, amelyhez szükséges egy privát kulcs, amelyből generálható a bitcoincím. A privát kulccsal annak tulajdonosa rendelkezhet, viszont fontos alapelv, hogy azt nem szabad senkivel megosztani. A privát kulcs pendrive-on is tartható, létezik továbbá mobiltelefonos pénztárca is.¹⁵ Léteznek már olyan bankfüggetlen vállalatok is (például Revolut), amelyek a hagyományos devizákon túl kriptodevizákkal is kereskednek, és szolgáltatásaik között megtalálható az elektronikus pénztárca, illetve a „prepaid” kártya (a prepaid kártya szolgáltatás egy előre meghatározott összeggel feltölthető bankkártya, amely bankszámla nélkül is igényelhető) funkciók is. Így már egy kvázi dombornyomott kártyán is lehet tartani a bitcoint.¹⁶

Ahhoz, hogy ezeket a virtuális fizetőeszközöket kényszerintézkedés alá lehessen vonni, megfelelő jogi szabályozás kiépítése szükséges, amely sokáig egyáltalán nem létezett, csupán annyit rögzítettek, hogy a kriptovaluták kereskedelméből származó nyereség után 15% adót kell fizetni.¹⁷ Ezzel kapcsolatban vezetett be újítást a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény 1. § *n*) és *o*) pontja, amelyek szerint e törvény hatálya kiterjed a Magyarországon székhellyel, fiókteleppel vagy telephellyel rendelkező virtuális és törvényes fizetőeszközök, illetve virtuális fizetőeszközök közötti átváltási szolgáltatásokat nyújtó szolgáltatóra, valamint letétkezelő pénztárca-szolgáltatóra. A törvény 3. § 22a) pontja értelmében letétkezelő pénztárca-szolgáltató: olyan szervezet, amely ügyfelei nevében virtuális fizetőeszközök tartására, tárolására és átadására szolgáló kriptográfiai magánkulcsok megőrzésével kapcsolatos szolgáltatást nyújt. A törvény 3. § 47. pontja rögzíti, hogy a virtuális fizetőeszköz nem más, mint digitális értékmegjelenítés, amelyet nem központi bank vagy közigazgatási szerv bocsát ki, illetve garantál; nem rendelkezik törvényes fizetőeszköz jogi státuszával; elektronikusan tárolható, csereértékként elfogadott, így különösen elektronikusan átadható, illetve elektronikus kereskedésre alkalmas.¹⁸

A fenti szabályozásból azt fontos rögzíteni a büntetőeljárás-jogi kényszerintézkedés szempontjából, hogy a kriptovaluták nem törvényes fizetőeszközök, és hogy elektronikusan tárolhatók. A büntetőeljárásról szóló 2017. évi XC. törvény (Be.)

¹⁵ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

¹⁶ HEGEDŰS-LÉNÁRD – UDVARY 2021: 11.

¹⁷ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

¹⁸ 2017. évi LIII. törvény 1. § *n*) és *o*) pontjai, 3. § 22a) pontja, 3. § 47. pontja.

315. § (2) bekezdése ezzel kapcsolatban úgy rendelkezik, 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 rendelkezési lehetőségét megakadályozza. A fizetésre használt elektronikus adat lefoglalását úgy lehet végrehajtani, hogy ezt a bitcoin azonosítási a szolgáló privát kulcsot el kell utalni egy hatósági címre, amihez a nyomozó hatóságnak is „hatósági pénztárcát” kell létrehoznia, hogy hozzáférjen a privát kulcs-hoz.¹⁹

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-BM-PM együttes rendelet (Rendelet) 67. § (5)–(6) bekezdései ezzel kapcsolatban úgy rendelkeznek, hogy az elkobzás vagy vagyonekobzás alá eső fizetésre használt elektronikus adat lefoglalását az új 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

- az adat vagyonekobzás alá esik, és a zár alá vétel feltételei nem állnak fenn, vagy az nem lenne végrehajtható, illetve
- az adat elkobzás alá esik, és az elektronikus adat ideiglenes hozzáférhetetlenné tételének vagy az elektronikus adat ideiglenes eltávolításának a feltételei nem állnak fenn.

Az új Be. 315. § (2) bekezdésében meghatározott művelet elvégzése végrehajtható olyan művelettel is, amely alapján a fizetésre használt elektronikus adat értékét a bűnjelkezelő e célból rendszeresített számláján írják jóvá.²⁰ Azonban a lefoglalás nem feltétlenül a legjobb megoldás, ugyanis az adathordozó lefoglalása nem garantálja, hogy azt a felhasználó (elkövető) nem tárolta máshol is.²¹

A Rendelet 67/A. § (1) bekezdése kimondja, hogy a lefoglalás végrehajtásához indokolt esetben szaktanácsadót kell igénybe venni.

A Rendelet 67/A. § (4) bekezdése akként rendelkezik, hogy a fizetésre használt elektronikus adat vagyonekobzás érdekében történő lefoglalását követően haladéktalanul fel kell hívni az érintettet, hogy a bűnjel előzetes értékesítése vagy megváltása kérdésében nyilatkozzon. Ha az érintett kéri a fizetésre használt elektronikus adat értékesítését, ez csak abban az esetben mellőzhető, ha arra a bizonyítás érdekében is szükség van.²² Ugyanis a Be. 319. § (1) bekezdése kimondja, hogy ha az eljárás során a lefoglalt dologra a bizonyítás érdekében már nincs szükség, hivatalból haladéktalanul meg kell vizsgálni, hogy a lefoglalás megszüntetésének van-e helye

¹⁹ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

²⁰ 11/2003. (V. 8.) IM-PM-BM együttes rendelet (Rendelet) 67. § (5)–(6) bekezdései.

²¹ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

²² Rendelet 67/A. § (5) bek.

vagy a lefoglalt dolog értékesíthető-e. A lefoglalt dolog akkor értékesíthető, ha a lefoglalt dologra a bizonyítás érdekében már nincs szükség.²³

A fenti szükséges jogszabály-ismertetést követően nézzük meg, hogy hogyan működik a gyakorlatban a kriptovaluták, azon belül is elsősorban a bitcoin felkutatása, lefoglalása. Az a személy, aki a bitcoint a saját címére fogadja – tekintettel arra, hogy a saját címét ismeri –, tisztában lesz a küldő címmel is a blokklánc nyilvánosságából fakadóan. Ez azt jelenti, hogy bármilyen – a blokklánc megtekintésére alkalmas – eszközzel ellenőrizhető, hogy az ő általa használt címre pontosan honnan is érkezett tranzakció. Ez egyben azt is jelenti, hogy ha a fogadó fél tisztában van a küldő személyével, úgy legalább egy hozzá tartozó bitcoincímet is ismerni fog. Ugyanez a gondolatmenet a bitcoint fogadó személy vonatkozásában is fennáll, azaz a fogadó – amennyiben előtte ismert a küldő személye – pontosan tudni fogja a forráscímről, hogy az kihez tartozik. A nyomozó hatóságok részére a fentiek azt jelentik, hogy amennyiben sikerül beazonosítani egy adott bűncselekményhez köthető bitcoincímet, majd az innen kimenő tranzakciókat nyomon követve egy természetes vagy jogi személyhez tartozó címre jutnak, úgy a címet használó személy vizsgálata mindenképp indokolt a büntetőeljárás során. Ilyen eset lehet, ha például ismertté válik egy internetes kábítószer-kereskedő által használt bitcoincím, és az onnan kiinduló utalások egy olyan címre jutnak, amelynek tulajdonosa valamilyen okból ismertté válik. Mindezek esetén egyértelmű kapcsolat merülne fel az ismeretlen kereskedő, illetve a blokklánc elemzése alapján a hozzá köthető kriptovalutával rendelkező személy között. A gyakorlatban nagyobb valószínűséggel fordul elő az a verzió, hogy valamilyen forrásból adat merül fel egy személyre, hogy az illető egy konkrét – virtuális fizetőeszköz alkalmazásával gyakran együtt járó – bűncselekménnyel – jellemzően kábítószer-kereskedelemmel – lehet összefüggésbe hozható. Ezt követően különböző nyílt, illetve leplezett eszközök alkalmazásával vizsgálható, hogy az illető rendelkezik-e bitcoinnal. Amennyiben igazoltá válik a személy vonatkozásában, hogy bitcoinnal rendelkezik, úgy szükséges megállapítani azt is, hogy a bűncselekményhez közvetlenül köthető cím hogyan hozható kapcsolatba az érintett vonatkozásában beazonosított címmel.²⁴ A tranzakciók személyhez és bűncselekményhez kötése sok esetben csak speciális nyomozási technikák – a magyar jogban úgynevezett leplezett eszközök – alkalmazásával kivitelezhető. Ez felöleli az online kutatást a kriptovaluta alkalmazásához szükséges adatok (wallet-fájl) és jelszavak felkutatása érdekében, az online fedett nyomozók igénybevételét, vagy az úgynevezett csapdaállítást.²⁵

Amennyiben a kimeneti címek ismertek, szükségünk van egy, a bűncselekményhez köthető bemeneti címre is. Ennek az adatnak a forrása szintén sokféle lehet, azonban ez jellemzően – a kábítószer-kereskedelem példánál maradva – egy az úgynevezett darkneten egykor elérhető darkmarket – azaz feketepiac – lesz. Ezek

²³ Rendelet 67/A. §-a, valamint a Be. 319. § (1)–(2) bekezdése.

²⁴ TÓTH et al. 2022: 99–100.

²⁵ POLT 2021: 424.

az internetes felületek ugyanolyan weboldalak, mint amelyeket mindennap használunk, azonban kizárólag egy speciális, védett és alapvetően lekövethetetlennek szánt hálózaton keresztül érhető el, ami a piacot működtetőknek, illetve az azon eladóknak és vásárlóknak is névtelenséget biztosít. Szintén az anonimitás érdekében ezek a szolgáltatók nem pénzt, hanem kriptovalutákat használnak a kereskedelmi tevékenység végzéséhez. Alapvetően a rendszer úgy néz ki, hogy az eladó regisztrál egy felhasználói nevet és jelszót a piacon, ahol a részére létrehoznak egy „számlát”, amely egy – a weboldal kezelésében álló – bitcoinpénztárca. Ugyanígy a vásárló is létrehoz egy felhasználói fiókot, és az ő részére is létrejön egy „számla”, ahová a saját bitcoincíméről utalja be az elkölteni szánt összegeket. A rendelés leadása során – általában titkosított kommunikációval – a vásárló megadja a postai címet, ahol a csomagot át kívánja venni, ezt követően a weboldal a vásárlás összegét a felhasználói fiókhoz tartozó számláról levonja, azonban az eladó részére csak akkor továbbítja, ha a vásárló visszajelzett a csomag átvételéről. Amennyiben ez a visszajelzés elmarad, vagy reklamáció érkezik, úgy – ha nem születik megegyezés a felek között – a feketepiac adminisztrátorai elbírálják az esetet, és döntenek arról, hogy a kérdéses összeg a vásárlóhoz kerül vissza, vagy az eladónak lesz kifizetve. Mindezek az üzenetváltások és kifizetések névtelenül történnek, de ez az anonimitás csupán addig garantálható, amíg az érzékeny információ birtokában lévő eladó számítógépe vagy a weboldalt tartalmazó szerver kényszerintézkedés hatálya alá nem kerül egy büntetőeljárás során. A névtelenség tehát valójában nem garantált. Ezt jól mutatja, hogy a közelmúltban több ilyen kereskedői felület is áldozatul vált többnyire az Egyesült Államok, illetve a nyugat-európai országok rendvédelmi szerveinek.²⁶

A büntetőeljárás során fel kell kutatni a privát kulcsot, amely aláírja a kérdéses tranzakciót. Ez a privát kulcs lehet akár mobiltelefonra telepített/letöltött alkalmazás is. Léteznek ugyanis olyan helyreállító kulcsok, amelyekkel a beérkező SMS-eket meg lehet tekinteni. Ezt követi a lefoglalás a kriptovaluta (bitcoin) azonosítása érdekében. Ehhez szükség van egy hatósági pénztárca létrehozására, ugyanis ennek segítségével lehet hozzáférni a privát kulcshoz. Létezik ugyanis egy 24 szavas helyreállító kulcs, amellyel vissza lehet állítani az elveszített adattartalmat. Felmerül a kérdés, hogy mit bizonyít a blokklánc? Lényegében az egyes bitcoincímek közötti tranzakciót, amely bonyolult matematikai műveletekből áll össze. A blokkláncon – amely mivel nyilvános, az elemzésére az interneten számos eszköz elérhető – egy BTC- (bitcoin-) tranzakció vonatkozásában a következő adatok láthatók: a tranzakció azonosítója (egy 64 karakterből álló sorozat); a küldő (forrás) bitcoincím vagy címek; a fogadó bitcoincím; a tranzakció ideje. Az említett bitcoincímeken valósul meg a BTC „tárolása”. Minden bitcoincímhez tartozik egy úgynevezett privát kulcs (*private key*), amelynek ismerete a címen található BTC elköltéséhez elengedhetetlen. Bárki, aki ezt a kulcsot ismeri, a bitcoint elköltheti, ezért is fontos, hogy egy esetleges lefoglalás során azonnal saját kezelésben lévő címre kell küldeni a lefoglalt

²⁶ TÓTH et al. 2022: 99–100.

összeget, mivel a kulcsról másolat is létezhet. Ez a kulcs gyakorlatilag megfejthetetlen, azonban ismeretében visszafejthető, megállapítható a bitcoin cím. A blokkláncon tehát bitcoin címek és tranzakciók láthatók. A helyreállító kulcs segítségével vissza lehet fejtetni a privát kulcsot, majd a blokkláncon ellenőrizzük, megnézzük a kérdéses tranzakciót, amelyet a privát kulccsal írtak alá. A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatala is rendelkezik egy hatósági bitcoin pénztárcával, amelynek segítségével a bankszámlák közötti tranzakciókat lehet nyomon követni.²⁷

A nyomozás vagy előkészítő eljárás során – amennyiben kriptodeviza alkalmazása a bűncselekmény típusa vagy más körülmények miatt felmerülhet – többek között a következőkre célszerű figyelemmel lenni:

A hitelintézetek felé küldött megkeresések kapcsán, a bankok által az elkövetői körhöz tartozó személyek számláival kapcsolatos adatkérésekre nyújtott válaszok között valamely virtuális fizetőeszköz-tőzsdére küldött vagy tőzsdéről való átutalást követően szükséges a tőzsde megkeresése is, mivel ott a pénzforgalom mellett vélhetően virtuális fizetőeszköz tranzakciója is történt, átváltás céljából. Ehhez természetesen a banki tranzakciós listákat elemezni kell, az ellenoldali számlaszámokról meg kell állapítani, hogy virtuális fizetőeszköz kereskedelmével foglalkozó gazdasági társasághoz vagy magánszemélyhez tartozik-e. A Készenléti Rendőrség Nemzeti Nyomozó Iroda eljárásában is jelentősége volt a bankszámla-információknak, mivel az egyik büntető ügyben a kábítószer-kereskedelemmel gyanúsítható elkövető testvére több alkalommal is fogadott pénzüsségeket a CoinCash Ltd. nevű gazdasági társaságtól, amely egy ismert hazai virtuális fizetőeszköz vásárlásával és eladásával foglalkozó gazdasági társaság. A céget az NNI megkereste, és válaszukban arról tájékoztattak, hogy az elkövetői körtől hogyan vásároltak virtuális fizetőeszközt (jelen esetben bitcoin). A tranzakcióval összefüggésben valamennyi, a blokkláncon található adatról tájékoztatást adtak, továbbá a váltást végző személyes adatairól is tájékoztattak. Amennyiben titokban történik a személy megfigyelése, akkor tekintettel kell lenni az olyan helyekre, ahol virtuális fizetőeszköz átváltásával foglalkozó gazdasági társasághoz köthető készülék, úgynevezett bitcoin-ATM van elhelyezve, vagy ezzel foglalkozó személy tevékenykedik.

Telefonos kommunikáció megfigyelése során figyelemmel kell lenni a kriptovalutákkal kapcsolatban alkalmazott kifejezésekre, illetve a bitcoin-ATM szolgáltatótól kapott szöveges üzenetekre.

A virtuális fizetőeszköz váltásával foglalkozó magyarországi vállalkozások felé adatkérést célszerű továbbítani az érintett személyes és egyéb ismert adatainak – például telefonszám, e-mail-cím – feltüntetésével.

A kutatás során az elektronikai eszközök, adathordozók vizsgálata, valamint a papíralapú feljegyzések áttekintése is szükséges, mivel többek között bitcoin-pénz-

²⁷ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás, valamint TÓTH et al. 2022: 95.

tárca, bitcoinpénztárcát helyreállító kód – *recovery seed* –, vagy virtuális fizetőeszköz váltására utaló böngészési előzmény is fellelhető lehet.

A kutatást olyan időpontban célszerű végrehajtani, amikor a célszemély számítógépe – nagy valószínűséggel – bekapcsolt állapotban található, hogy az ott tárolt adatokhoz együttműködő magatartás hiányában is hozzájuthassunk. A cél ebben az esetben a privát kulcs megszerzése és egy tranzakció végrehajtása a hatóság által kezelt pénztárcába. Kiemelendő, hogy a virtuális fizetőeszközöket nem az eszközön tárolják. A pénztárca csupán a privát kulcsot tárolja, amely az elköltéshez kell. A pénztárcák között megkülönböztetünk szoftveres, hardveres, nyomtatott és online pénztárcákat.

A szoftveres pénztárca olyan számítógépes vagy mobiltelefonos alkalmazások összessége, amelyek többnyire egy grafikus felületen keresztül kommunikálnak a felhasználóval, és lehetővé teszik a virtuális fizetőeszköz egyenlege, a címek, a tranzakciók megtekintését, illetve virtuális fizetőeszköz küldését vagy fogadását. A leggyakrabban használt ilyen alkalmazás Bitcoin esetében az Electrum nevű program. Több olyan alkalmazás is létezik, amely nemcsak bitcoin, de akár más virtuális fizetőeszközök privát kulcsainak tárolására is alkalmas, ilyen például a JAXX. Az alkalmazások általában hasonló felhasználói felülettel rendelkeznek, ezért az eszközök átvizsgálását végrehajtó eljárónak célszerű megismerkednie legalább egy ilyen szoftver működésével. Szintén fontos az eszközök már a helyszínen való átnézése ilyen szoftverek után kutatva.

Aszoftveres pénztárcáknál biztonságosabb tárolási lehetőséget nyújtanak az úgynevezett hardveres pénztárcák, mint a Ledger, Trezor vagy a KeepKey. Ezek USB-porton számítógéphez csatlakoztatható eszközök, amelyek titkosítottan tárolják a virtuális fizetőeszközök privát kulcsait, akár egyidejűleg többfélét is. Ezek az eszközök PIN-kóddal védettek, ezért hozzáférni – a kód ismeretének hiányában – csak a tulajdonos együttműködésével lehetséges. Az ilyen pénztárcák esetén egy számítógépes szoftver is szükséges a küldéshez, fogadáshoz, azonban a biztonság szempontjából nagyon fontos funkció, hogy a tranzakció jóváhagyását magán az eszközön egy gombnyomással vagy PIN-kód beírásával kell végrehajtani.

A helyreállító kulcsnak, vagy *recovery seed*nek az úgynevezett determinisztikus pénztárcák esetén van jelentősége. Mind a hardveres pénztárcák, mind a legtöbb szoftveres pénztárca alkalmaz *recovery seed*-et. Ez azt jelenti, hogy a tárca létrehozásakor generál egy 12 vagy 24 szóból álló listát, amelyet le kell jegyezni, mert az eszköz megsemmisülése esetén ez alapján a teljes pénztárca visszaállítható lesz. Ez úgy lehetséges, hogy a szavak által megtestesített kódból egy matematikai eljárással generálják a privát kulcsokat és a címeket, amelyek hozzáférést biztosítanak az összegekhez.

Lehetőség van a privát kulcs papíralapú kinyomtatására (nyomtatott pénztárca) is, amelyhez több alkalmazás is biztosít eszközt, mint például a bitaddress.org. Ezen a privát kulcs titkosítás nélkül látható, ezért azt megmutatni senkinek nem szabad. A nyomozó hatóság célja a privát kulcs megismerése, ezért amennyiben ilyen paper

wallettel találkozik a nyomozati szerv, az ott található összeget az Electrum alkalmazásba való bemásolással a nyomozó hatóság eljáró tagja elküldheti saját, hatósági pénztárcájába.

A számítógépen, mobiltelefonon az említett alkalmazások mellett figyelemmel kell lenni böngészési előzményekre, képfájlokra, szöveges fájlokra, e-mailekre, mivel azok virtuálisfizetőeszköz-tőzsdékre utaló adatokat, más virtuális fizetőeszköz tranzakcióira utaló információkat, vagy akár recovery seedeket tartalmazhatnak. Ugyanez természetesen a papíralapú feljegyzésekre is igaz. A Készenléti Rendőrség Nemzeti Nyomozó Iroda saját eljárása során nagy segítséget jelentett, hogy a fogva tartott kábítószer-kereskedő részletes instrukciókat adott a családtagok irányába, és leveleiben többek között azt is tudatta, hogy milyen kriptodevizából mekkora mennyiséggel rendelkezik, sőt gyakran azt is leírta, hogy melyik hardveres pénztárcán vagy melyik alkalmazásban tárolja azokat.

A büntetőeljárásról szóló 2017. évi XC törvény 315. § (2) bekezdése kialakította a virtuális vagyontárgyak biztosításának keretszabályait, amely alapján a virtuális fizetőeszközök lefoglalása végrehajtható: „A fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan művelet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.” Ez praktikusán annyit jelent, hogy amennyiben egy, a „Bitcoin a nyomozás során” részben említett kutatás folyamán virtuális fizetőeszköz – azaz fizetésre használt elektronikus adat – lefoglalása válik indokolttá, azt célszerű a lehető leghamarabb úgy végrehajtani, hogy a megismert privát kulcs használatával a címeken található teljes összeget egy, a hatóság kezelésében álló bitcoin- vagy más virtuálisfizetőeszköz-címre utalják át, hogy az érintett személy semmiképp ne rendelkezessen a lefoglalás tárgyával.

Tekintettel arra, hogy a Be. 36. § (2) bekezdése szerinti, a bűnjel és a bűnügyi vagyon kezeléséért felelős szerv még nem működik, valamint letéti számlára a 11/2003 (V. 8.) IM-BM-PM együttes rendelet alapján csak lefoglalt pénz fizethető be – a virtuális fizetőeszközök pedig nem azok –, a hatóság kezelésében álló bitcoin-címet alapvetően a lefoglalást végrehajtó hatóságnak kell létrehoznia, ahová a lefoglalt összegek mozgathatók. Hatósági pénztárcának a legalkalmasabb eszközök a Ledger (vagy más hardveres pénztárcagyártók) által előállított készülékek, biztonságukra tekintettel.

Amennyiben a lefoglalás a kutatás során a helyszínen történik, úgy a kutatásról készített jegyzőkönyvben kell feltüntetni a végrehajtott tranzakciókat, illetve azok legfontosabb ismérveit, azaz, hogy milyen pénztárcatípusból vagy milyen helyreálítási kulcs alkalmazásával mikor, milyen tranzakciós azonosítóval, mekkora mennyiségű és milyen virtuális fizetőeszközt továbbítottak a hatóság által működtetett pénztárcába. Amennyiben a lefoglalás nem a helyszínen, nem az érintett jelenlétében történik, hanem úgy, hogy a lefoglalt egyéb adatok, feljegyzések átvizsgálása során sikerül a virtuális fizetőeszközhöz hozzáférést szerezni, akkor a Be. 361. § (6) bekezdése alapján feljegyzés is készíthető a halasztást nem tűrő eljárási cselekményről.

Ha a virtuális fizetőeszköz privát kulcsát nem maga az érintett személy tárolja, hanem valamely virtuális és törvényes fizetőeszközök közötti átváltási szolgáltatót vagy letétkezelő pénztárca-szolgáltatót vesz igénybe (online pénztárca), úgy nincs lehetőség a közvetlen, nyomozó hatóság általi lefoglalásra, hanem a virtuális fizetőeszköz kezelő szolgáltatónál kell kezdeményezni az érintett számlájának zár alá vételét, illetve tartalmának lefoglalását. Az érintett nevében a nyomozó hatóság tehát nem adhat megbízást tranzakció végrehajtására harmadik félnek.²⁸

Az internetes nyomozás és realizálásra, a bitcoinok tranzakcióelemzésére, a kábítószer-kereskedők azonosítására, valamint a postai realizálás szoros összefüggésére mutatnak rá az alábbi jogesetek. Egy 2012-ben végrehajtott rajtaütési akció során a szlovák rendőrség segítségével felderítettek és elfogtak egy olyan forgalmazót, aki az interneten keresztül forgalmazott nagy mennyiségben új pszichoaktív anyagokat, illetőleg kábítószer (4-MEC). Az anyagokat Szlovákiában csomagolták, és egy csomagküldő szolgálat révén juttatták el a magyarországi megrendelőkhoz.²⁹

Egy másik példaként lehet felhozni a Porto műveletet, amelynek keretében 2017 májusában az osztrák és német bűnüldöző hatóságok befejezték a rajtaütést. Ennek során célba vették a tiltott kábítószerekkel kereskedő vásárlókat és eladókat a darknetes piacokon. A művelet eredményeként 697 nyomozás indult az egyes gyanúsítottak ellen, valamint 35 kg különféle kábítószer lefoglalására került sor Ausztriában. A művelet rávilágít a darknetes felületen zajló kábítószer-kereskedelem és csomagcsempészet közötti szoros összefüggésre. A művelet részeként végrehajtott ellenőrzési tevékenységek eredményeként Németországban 6000 csomagot foglaltak le, amelyek több mint 175 kg kábítószeret tartalmaztak. A csomagok címzettjei 60 országban működtek világszerte.³⁰

Harmadik példaként említhető az AlphaBay nevű darknetes kábítószer-kereskedő oldal, amelyet 2018-ban sikerült lefoglalnia az Europolnak. Az AlphaBay nevű oldalon árusított kábítószeres esetében Magyarországon gyártották a tablettákat. A fogdafelderítés során látott napvilágot, hogy az elkövetőnek van privát kulcsa az oldalhoz, amelyet a cellatársai használtak. A felderítés során kiderült, hogy az elkövető a kábítószer-kereskedelemből származó bűnös bevételeket kondicionáló termékekbe, drága személygépkocsikba fektette, továbbá felújításokra fordította. Az elkövető AlphaBay nevű darknetes oldallal való kapcsolatát a blokkláncelemzés, a bitcoincímek kinyerése segítette elő. Az elemzés rámutatott arra, hogy az elkövető erről a darknetes oldalról szerezte a vagyonát, ezért az oldalt az Europol lefoglalta. A blokkláncelemzés, a bitcoinfőkönyvek elemzése révén el lehet jutni a vásárlóktól a kereskedőkhöz, azaz A címétől B címéig, akik az ügyletekből busás nyereségre tettek szert. A felderítés sikerességét hivatott alátámasztani, hogy bitcoin mellett,

²⁸ TÓTH et al. 2022:104–122.

²⁹ CsÁK et al. 2013: 98.

³⁰ EMCDDA 2017: 60.

más kriptovalutát, így ethereumot is sikerült lefoglalni, valamint bányászatra alkalmas nagy teljesítményű számítógépeket is.³¹

A tranzakcióelemzés segítségével tehát azonosíthatók a kereskedők, és a postai úton kiszállított kábítószert vagy új pszichoaktív anyagot tartalmazó csomagok útja is.

Összegzés, kitekintés, de lege ferenda javaslatok

Ki kell dolgozni a kriptovalutákkal kapcsolatos kényszerintézkedések módszertani utasítását, valamint azok értékesítésének módját. Stratégiai szinten jó tudni, hogy a visszaélések nem elkerülhetők egy-egy ország jogalkotásának, végrehajtó hatalmának elszigetelt megoldásaival. Szükséges az átfogó szabályozás. Erre azonban meglehetősen kicsi az esély, hiszen mindig vannak ellenérdekeltek felek és kapcsolódó nem kívánt hátrányok. Ha csak arra gondolunk, hogy a rendészeti szervek sok éves küzdelem után sem tudták elérni, hogy legyen egy egységes bankszámla-nyilvántartás belföldi pénzintézetekről, akkor elég csekély annak az esélye, hogy életre hívható egy regiszter arról, milyen kriptovalutával kapcsolatos szolgáltatók működnek a világban, és kik az ügyfeleik. Egyre valószínűbb, hogy nem lehet megakadályozni a kriptovaluták fokozott térnyerését a pénzügyi szektorban. Egymással szemben áll azonban két állami/társadalmi érdek: az innovatív technológiák szárnyalásának lehetővé tétele és a vagyonmozgások átláthatóságának, korlátozhatóságának érdeke. Minden bizonnyal azokon a pontokon lehetséges megteremteni a kriptovaluták átláthatóságát, ahol a hatósági ellenőrzés és felügyelet alatt álló pénzügyi szolgáltatók és személyek megjelennek. Ha olyan szabályozás kidolgozására kerülne sor, amely szerint egy vállalkozás (bizonyos limit felett) csak akkor érhet el profitot a kriptovalutákból származó ügyletből (kriptopénzváltók, onlinetárca-szolgáltatók, kriptopénz-ATM-üzemeltetők stb.), hogyha az ügyfelét beazonosította, az jelentős korlát volna azzal szemben, hogy a kriptopénzeket a bűnös vagyon eredetének elrejtésére, legalizálására vagy felhasználására alkalmazzák. Ezek a rendelkezések a pénzmosás elleni normákból is következnenek, de ezek betartatása, kikényszerítése jelenleg nem történik meg. A kriptovaluták sorsát jelentős részben a kapcsolódó jogi szabályok határozzák meg, azaz hogy az egyes államok milyen mértékben tiltják, korlátozzák a használatukat. A kriptovalutákat nagy arányban használják bűncselekmények elkövetéséhez, illetve bűnös forrásból származó javak mozgására, elrejtésére. Simon Béla véleménye szerint bizonyosan maradnak olyan államok – jellemzően offshore területen –, amelyekben a kriptovaluták konvertibilis valutákra való átváltása megoldható marad, így nem vonhatók ki a kriptovaluták a pénzmosás eszköztárából. Sokkal célszerűbb szélesebb körben lehetőséget adni nekik, és a saját jogrendsze-

³¹ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

rünkben a törvényes és ellenőrizhető működés keretein belül tartani. A tiltásokkal és súlyos korlátozásokkal ellentétben célszerűbb az enyhe korlátozások és szabályozott keretek megteremtése. Hasonlóan a kriptográfiai megoldásokhoz vagy a torlázathoz: a szellemet nem lehet visszazárni a palackba, így meg kell próbálnunk kordában tartani és a lehetőségekhez mérten felügyelni.³²

A probléma továbbra is a tranzakciók elkövetőhöz és bűncselekményhez kapcsolása, illetve mindezek időszerű megállapítása. Ez nem oldható meg csupán a technológiai eszközök szintjén, ehhez kikényszeríthető szabályozás kell. A kriptovaluta átalakítása, a bűncselekménnyel és elkövetőkkel való kapcsolat azonosítása a fizetési rendszer be- és kilépési pontjain oldható meg, azaz akkor, amikor a kriptovalutát hagyományos pénzre váltják át és vissza. Jogi oldalon az Európai Parlament és Tanács 2018/843-as irányelve a pénzmosás elleni küzdelem jegyében meghatározza a virtuális letétkezelő pénztárca-szolgáltató fogalmát. Eszerint letétkezelő pénztárca-szolgáltató: „olyan szervezet, amely ügyfelei nevében virtuális fizetőeszközök tartására, tárolására és átutalására szolgáló kriptográfiai magánkulcsok megőrzésével kapcsolatos szolgáltatást nyújt.” Az irányelv a letétkezelő pénztárca-szolgáltatót és az átváltási szolgáltatásokat nyújtó szolgáltatókat is kötelezi a pénzügyi intézményekre előírt pénzmosás-megelőzési szabályok alkalmazására. A cél, hogy megszűnjön a tranzakciók anonimitása az Európai Unióban bejegyzett és az irányelv hatálya alá tartozó szolgáltatók igénybevétele esetében.³³

A megfelelő polgári jogi kategóriák hiányában a magyar büntetőeljárás szabályok kiindulópontja a kriptovaluták digitális léte, azaz a szabályozás számítástechnikai adatokkal való műveletek végzésére épül. E rendszerben a kriptovaluta vagyoni értéket megtestesítő számítástechnikai adat, amelyet fizetésre használnak. A magyar büntetőeljárás jog a hiányzó vagyonjogi szabályozás kiküszöbölése érdekében a magánjogi dogmatikát tiszteletben tartva kodifikálta a virtuális valuták lefoglalásának szabályait, ezzel tulajdonképpen már ekkor egyfajta jogi státuszt adott a jelenségnek. A sikeres lefoglalás után a vagyonelkobzás eredményeként a kriptovaluta tulajdonjoga az államra száll, ami feltételezi az állami kriptovaluta-tárcák fenntartását vagy a kriptovaluta átváltását nemzeti valutára. Mindez megint csak kivitelezhető technológiailag: a nyomozó hatóság biztonságos tárolóeszközöket (úgynevezett *ledger*) szerzett be.³⁴ Ugyanakkor szükséges létrehozni a bűnügyi vagyon kezeléséért felelős szervet, valamint egy olyan letéti számlát, ahová a büntetőeljárás során lefoglalt virtuális fizetőeszközöket is be lehet fizetni, és át lehet váltani az adott ország nemzeti valutájára. Olyan további kérdések rendezése is szükséges, hogy a jogi státusszal nem rendelkező vagyon lefoglalása megalapozhat-e kártalanítási igényt, mivel a kriptovaluta az árfolyamának változása következtében akár jelentősen is veszíthet a reálértékéből. Ezt a magyar szabályozás az úgynevezett előzetes értékesítés szabályrendszere szerint tudja megoldani. A büntetőeljárás kényszerintézkedések

³² SIMON 2018: 86–87.

³³ POLT 2021: 424; továbbá Az Európai Parlament és a Tanács (EU) 2018/843 irányelve.

³⁴ POLT 2021: 425–426.

kialakításához ezért is lenne szükség a minimális polgári jogi dogmatikai alapok megteremtésére, hogy ez minél körütekintőbb módon történjen.³⁵

Ezért a dolog fogalmát a bitcoinra és a többi kriptovalutára is szükséges lenne kiterjeszteni annak érdekében, hogy le lehessen foglalni, illetve hogy elkobzás, vagyoneklobzás alá lehessen vonni, amennyiben azt bűncselekménnyel összefüggésben szerezték. Például akként, hogy a tulajdonjog tárgyait a dolgokon túl a forgalomképes, de nem dologi természetű javakra is kiterjesztik, vagy amelyek a dolog fogalmát terjesztik ki immateriális javakra (testetlen dolgokra).³⁶ Ennek elméleti alapját a Btk. 76. §-ban foglalt értelmező rendelkezés megteremti, amikor kimondja, hogy a vagyoneklobzás alkalmazásában vagynonon annak hasznát, a vagyoni értékű jogot, követelést, továbbá bármely, pénzben kifejezhető értékkel rendelkező előnyt is érteni kell. A kriptovaluta tehát büntetőjogilag értékelhető vagyonelemnek minősül Magyarországon is, így vagyoneklobzás alá eshet.³⁷

Továbbá ki kell dolgozni a megfelelő polgári és pénzügyi jogi szabályozást annak érdekében, hogy milyen feltételek mellett használható legálisan a bitcoin, az értékállósága vonatkozásában pedig fontos lenne az árstabilitás biztosítása a fedezet nélküli pénzkibocsátás elkerülése miatt. Mindezekon túlmenően megfontolandó e kriptovalutáknak a pénzügyi piaci, monetáris szabályozás alá vonása is, hogy kontrollt lehessen gyakorolni e kriptovaluta adásvétele felett, mivel pénzkibocsátási monopóliuma egyedül a központi bankoknak van. Másrészt adójogi szabályozás révén (például a bányászatot végző magánszemély a kitermelt bitcoinból származó jövedelmet köteles az összevont adóalapba beszámítani mint önálló tevékenységből származó jövedelmet) megakadályozni a teljes vagyon kimentését, elrejtését. Magyarországon nincs tehát olyan átfogó gazdasági, illetve pénzügyi jogi szabályozás, amely közvetlenül a kriptovalutákra vonatkozna. Közvetve azonban megjelent az adózásra vonatkozó szabályok között: 2022. január 1-jétől az évi költségvetéssel párhuzamosan kialakított adójogi szabályok részeként a személyi jövedelemadóról szóló törvény külön szakasza foglalkozik a kriptovalutákkal: a bányászatból és kereskedésből származó haszon után csupán a 15%-os személyi jövedelemadót kell megfizetni. Az Európai Unióban jelenleg is zajlik a Crypto Asset Regulation kidolgozása, amely uniós szinten szabályozná a kriptoeszközök piacát. A közös piac, a tőke szabad áramlása miatt feltételezhető, hogy a magyar szabályozás bevárja az uniós jogalkotást.³⁸ Annak érdekében, hogy e kriptovalutákat is végrehajtás alá lehessen vonni, szükséges lenne egy olyan szabályozás bevezetése, amely előírná, hogy ezeket a kriptovalutákat is csak pénzforgalmi szolgáltatónál lehet kezelni és szükséges ezeket átváltani az adott ország nemzeti valutájára, illetve más devizára. A cél a bűnös úton szerzett vagyonelemeknek a vagyon-visszaszerzési eljárás keretében való visszaszerzése. Ennek érdekében fontos az együttműködés az EU-ban működő

³⁵ POLT 2021: 426.

³⁶ MENYHÁRD 2010: 37.

³⁷ POLT 2021: 423; valamint Btk. 76. §.

³⁸ POLT 2021: 421.

vagyon-visszaszerzési hivatalokkal az ARO/CARIN irodákon, valamint a JIT-eken keresztül, annál is inkább, mivel Magyarországon az ingó vagyonelem tekintetében éves szinten 2%-os a vagyonelemek sikeres visszaszerzése.³⁹

A kriptovalutákra vonatkozó megfelelő polgári jogi, pénzügyi jogi szabályozás kidolgozása fontos lenne a végrehajtási eljárás szempontjából is, mivel a Vht. 15. § (1) bekezdésének *b*) pontja akként rendelkezik, hogy az elsőfokon eljáró bíróság végrehajtási lapot állít ki a bíróság büntetőügyben hozott határozatának a polgári jogi igénynek helyt adó rendelkezése alapján, valamint a büntetőeljárásban részt vevő személy részére büntető költség megállapításáról szóló rendelkezése alapján.⁴⁰

A jelenlegi jogszabályi keretet figyelembe véve és szigorúan elméleti síkon maradva, ha értékközvetítő eszközként, szűkebb értelemben pénzként tekintünk a bitcoinra, úgy a bírósági végrehajtásról szóló 1994. évi LIII. törvény (Vht.) szabályait az alábbiak szerint kellene rá alkalmaznunk – ha ez lehetséges. Ugyanis a bitcoin kétséget kizáróan rendelkezik a pénz 3 fő tulajdonsága közül kettővel. Értékközvetítő szerepet tölt be, hiszen más csereeszközök értékének megállapítására alkalmas elszámolási egység, továbbá eladható eszközről beszélünk, mivel a tulajdonosa – az azt elfogadó közösség tagjai között – bármikor, bárhol könnyen beválthatja, vagyis rendelkezik a készpénzre jellemző nagy fokú likviditással. Az értékállósága már megkérdőjelezhető, mivel nagymértékű ingadozáson megy át napi szinten is, azonban hosszú távú értéknövekedését nézve láthatjuk, hogy folyamatosan emelkedik az ára. Amennyiben készpénzként tekintünk rá, a Vht. 100. §-a rendezi a készpénz lefoglalásának speciális szabályait. E szakasz értelmében a végrehajtó a lefoglalt készpénzt magához veszi, és a foglalást követő munkanapon befizeti a végrehajtói letéti számlára. E foglalási lehetőség azonban kiesik a lehetséges eszközök közül, tekintettel arra, hogy a bitcoin nem kézzelfogható értéktárgy, nincsen fizikai megjelenése, így a végrehajtónak nincsen lehetősége arra, hogy a helyszínen azt birtokba vegye, majd befizesse annak ellenértékét a letéti bankszámlaszámra. Amennyiben tovább kutatunk a Vht. rendelkezései között, úgy a számlapénzre vezetett végrehajtás szabályai jöhetnek még szóba a vagyontárgy megjelenési formája miatt. Azonban már itt is az elején megakadna a végrehajtási folyamat, mivel a Vht. 82/A. § (1) bekezdése úgy kezdődik, hogy a pénzforgalmi szolgáltatónál kezelt, az adós rendelkezése alatt álló vagyonelemet tud a végrehajtó foglalni. Ennek oka az, hogy a közvetítő harmadik fél közreműködése elengedhetetlenül szükséges a végrehajtói intézkedés foganatosításához. Azonban a bitcoin rendszere (P2P rendszer) kizárja a megbízott harmadik fél létét e jogviszonyban, így helyette a teljes online felhasználói közösséget kellene a végrehajtónak megkeresnie az utasítás végrehajtása érdekében. Ha a joghatósági problémáktól el is tekintenénk,⁴¹ ez a gyakorlatban nem lenne működőképes lépés,

³⁹ A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.

⁴⁰ Vht. 15. § (1) bekezdés *b*) pontja.

⁴¹ A Vht. alapján kizárólag a Magyarországon fekvő vagyonelemek tekintetében van mód a végrehajtás foganatosítására, Magyarországon honos pénzintézetek kereshetők meg az általuk vezetett követelések lejelentésére.

mivel nincs konkrét címzett az utasítás teljesítésére, illetve nincs olyan személy, akit kötelezhet és szankcionálhat a végrehajtó a teljesítés megtagadása esetén.

További problémaként merül fel, hogy a decentralizált főkönyvi nyilvántartás láthatatlan a hatóságok számára, és az anonimizált rendszere miatt kideríthetetlen a tulajdonosok személye. Amíg a bankok a számlatulajdonosok adatait kezelik, közlik például egy hatósági megkeresés alapján, addig a bitcoin esetén a rendszer a tárca azonosító kódját tartja nyilván, és az azon szereplő összeget, amiből nem lehet visszavezetni, hogy ki az adott tárca tulajdonosa, így nincs személyhez köthető beazonosítható vagyonelem, amelyre az eljárást le lehetne folytatni. További nehézség, hogy az elektronikus pénztárca a digitális térben létezik. Abban tárolt bitcoinhoz a végrehajtó csak abban az esetben tudna hozzáférni, ha megszerzi a wallethez tartozó privát kulcsot, amelyet csak a tárca tulajdonosától lehetne bekérni mint adatot. Itt azonban felmerülhet egy olyan rendhagyó eset is, amikor az adós a bitcoincímét és a hozzá tartozó privát kulcsot offline módon, azaz kinyomtatva az otthonában őrzi. Ebben az esetben a kinyomtatott pénztárcaadatok QR-kód formájában rendelkezésre állnak, amelyeket mobiltelefonon keresztül könnyen be lehet olvasni, ami által már elérhetővé is válnak a virtuális érmék. Azonban ahhoz, hogy a bitcoin értékét a végrehajtó forintban le tudja foglalni, át kell váltani a BTC-t, amit az erre létrehozott automatákból tud megtenni. Az átváltást követően a végrehajtó a forintban rendelkezésre álló összeget már be tudja fizetni a végrehajtó letéti bank-számlaszámára, így ebben a formában a Vht. 100. §-ban rögzített foglalási mód alkalmazható lenne.

Amennyiben az adós online módon tárolja a bitcoinját, úgy alkalmazni lehetne a Vht. által alapelvei szinten rögzített adósi együttműködési, bejelentési kötelezettséget, amelynek alapján, ha a végrehajtó az eljárása elején az adóst a tartozás haldéktalan megfizetésére felszólítja, azzal párhuzamosan az ilyen jellegű vagyontárgyának a bejelentésére is kötelezi. Másik oldalról nézve pedig maga a végrehajtást kérő is bejelentheti az eljárás során bármikor, hogy tudomása van arról, hogy az adós rendelkezik ilyen vagyontárggyal, amelynek, ha bejelenti a privát kulcsát, úgy a végrehajtó tudna intézkedni annak értékesítése iránt. Az adósi közreműködés elmaradása rendbírsággal lenne szankcionálható, ami a gyakorlatban nehezen elképzelhető, mert sem a végrehajtó, sem a bíróság nem tudná ellenőrizni, vagy ellenőriztetni hatósági erővel, hogy az adós valóban rendelkezik-e, vagy már nem rendelkezik ilyen privát kulccsal.

Egy másik megközelítési mód lehetne a társszervekkel (adóhatósággal) való szorosabb együttműködés kapcsán a hatósági bejelentés, adatközlés. Az adójogi szabályozás rögzíti, hogy a bányászatot végző magánszemély a kitermelt bitcoinokból származó jövedelmet köteles az összevont adóalapba beszámítani mint önálló tevékenységből származó jövedelmet. Ha az adós ilyen bejelentést tett, és ezt a végrehajtóval törvényesen közölni lehet, hogy az adózás időpontjában rendelkezett ilyen vagyonelemmel, a felszólítást meg lehet tenni az adós felé. Más kérdés, hogy a teljesítés, közreműködés elmaradása nehezen lenne szankcionálható. Mindezek alapján

a hatályos jogszabályok szerint felvetett lehetőségek mindegyike alkalmatlan lenne a bitcoin mint vagyonelem lefoglalására. Így, ha változatlan maradna a jogszabályi környezet és az évek múlásával a kriptovaluták népszerűsége is töretlen maradna, úgy lenne olyan kimentési lehetőség az adósoknak, amelyen keresztül a vagyonukat hatékonyan el tudnák rejtetni a hitelezők elől.⁴²

Irodalomjegyzék

- CSÁK Róbert et al. (2013): *2013-as éves jelentés az EMCDDA számára*. Nemzeti Drog Fókuszpont. Online: http://drogfokuszpont.hu/wp-content/uploads/EMCDDA_jelentes_2013_HU1.pdf
- DORNFELD László (2021): A kriptovaluták és az e-bizalom kapcsolata. *Magyar Rendészet*, 21(4), 211–227. Online: <https://doi.org/10.32577/mr.2021.4.12>
- EMCDDA (2017): *Drugs and the Darknet. Perspectives for Enforcement, Research and Policy*. Luxembourg: Publications Office of the European Union. Online: <https://doi.org/10.2810/783427>
- HEGEDŰS-LÉNÁRD Erika – UDVARY Sándor (2021): Kriptovaluta a vagyonban a végrehajthatóság tükrében. Kezdeti lépések a bitcoin foglалása felé. *Executio*, 10(1), 8–14.
- A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatal nyomozói által 2022. február 16. és február 17. között megtartott online konferencián elhangzó szakmai előadás.
- MENYHÁRD Attila (2010): *Dologi jog*. Budapest: ELTE Eötvös.
- POLT Péter (2021): A 21. század kihívásainak hatása a büntetőeljárásra. Kriptovaluták, azaz az új vagyoni értékek büntetőjogi kérdései. In BARABÁS A. Tünde – CHRISTIÁN László (szerk.): *Ünnepi tanulmányok a 75 éves Németh Zsolt tiszteletére*. Budapest: Ludovika. 419–427.
- SIMON Béla (2018): Kriptovaluták – rendészeti válaszok. *Belügyi Szemle*, 66(10), 71–87. Online: <https://doi.org/10.38146/BSZ.2018.10.5>
- TÓTH Zsolt et al. (2022): *Módszertani útmutató a bűnös úton szerzett vagyon felkutatásához és biztosításához*. Készült a Belső Biztonsági Alap, BBA-5.3.3/3-2017-00004 számú Kompetencia-fejlesztés, szakmai képzések lebonyolítása c. program keretében.

Jogforrások

1994. évi LIII. törvény a bírósági végrehajtásról
2012. évi C. törvény a Büntető Törvénykönyvről
2017. évi XC. törvény a büntetőeljárásról
2017. évi LIII. törvény a pénzmosság és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról
- 11/2003. (V. 8.) IM-PM-BM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról
- Az Európai Parlament és a Tanács (EU) 2018/843 irányelve a pénzügyi rendszerek pénzmosság vagy terrorizmusfinanszírozás céljára való felhasználásának megelőzéséről szóló (EU) 2015/849 irányelv, valamint a 2009/138/EK és a 2013/36/EU irányelv módosításáról

⁴² HEGEDŰS-LÉNÁRD – UDVARY 2021: 12–14.

ABSTRACT

The Emergence and Spread of Cryptocurrencies and Possible Legal Responses to the Phenomenon

Gellért JÁMBOR

One of the most important characteristics of money – as an official medium of exchange – is that the state is responsible for its issuance and, through the determination of the quantity of the emission, also the determination of its value. The right to issue money in Hungary is exercised by the state through the Hungarian National Bank. Cryptocurrencies, on the other hand, are reminiscent of the early phase of the development of money, they function as a free medium of exchange in a transaction that can be evaluated under civil law. The state has no influence either on their emission or on their inclusion, nor on inflating or deflating their value through the determination of the quantity. It is important to note that the exemption of cryptocurrencies from monetary regulation often means that they can serve as an exchange value for prohibited legal transactions that would otherwise be prohibited by law, e.g. financing of terrorism, distribution of drugs or other illegal substances. Cryptocurrency includes all digitally created funds that have been created through cryptographic encryption, “hashing”. And hashing is a digital process that can compress an arbitrary data stream to the specified size using an irreversible mathematical operation. The aim of the study is to show what kind of challenge cryptocurrencies pose to legal practitioners due to the fact that they are not subject to cash flow regulation, what kind of legal regulation is possible in the face of this new phenomenon, and in which areas of law it would be necessary to implement a further legislative process.

Keywords: *cryptocurrencies, encryption, blockchain analysis, seizure*