NAGY ÁGNES

Bitcoin a büntetőeljárásban

Bevezetés

A rendelkezésre álló adatok alapján megállapítható volt, hogy X.Y. és Z.Zs. kábítószer-előállítással és -kereskedelemmel foglalkoztak, amelyből illegális vagyonra tettek szert. A kereskedelmi tevékenység nagy része a darkneten zajlott, egy *„Csillag”* nevű felhasználóhoz köthetően.
Az elkövetési időszakban a darkwebes kereskedő a kábítószert egy közismert netes piactéren árusította, melynek ellenértékét a vásárlók bitcoinban (BTC) fizették.

X.Y. és Z.Zs. az illegálisan szerzett vagyon kimentését, illetve legalizálását a családjuk segítségével végezték. A kábítószer-kereskedelemből és az ahhoz köthető egyéb bűncselekményekből nagyságrendileg a büntetőeljárás kezdetekor releváns árfolyam alapján kb. 800 millió Ft-os vagyont halmoztak fel, ami az elsődleges információk szerint BTC-ban állt rendelkezésre. A bitcoin technikai kezelésével kapcsolatban Z.Zs. rendelkezett nagyobb ismerettel, azonban büntetés-végrehajtási intézetben tartózkodott a pénzmosás elkövetésekor is, ezért külső hozzáférést kellett biztosítania rokonai révén a felhalmozott vagyonhoz.

K.K. megalapozottan gyanúsítható a Btk. 399. § (1) bekezdés a) pont aa) alpontjába ütköző és aszerint minősülő, különösen nagy értékre elkövetett pénzmosás bűntett elkövetésével. Érintettsége vonatkozásában megállapítható, hogy Z.Zs. után második számú személyként vett részt a cselekményben, külön utasítások alapján főként K.K. tevékenysége révén realizálódott a bitcoinban és egyéb kriptovalutában tárolt pénzösszeg Magyarországon. Tevékenyen szervezte, és barátnője bevonásával leplezte a pénzváltásokat, vállalkozási szándéka is volt, illetőleg a kriptovalutában tárolt vagyon eredetéről tudomással bírt.

Kiváló tevékenysége eredményeképpen közreműködött 80 millió forintnyi összeg bitcoinból történő átváltásában és a pénzösszegek tovább utalásában.

L.L. szintén megalapozottan gyanúsítható a Btk. 399. § (1) bekezdés a) pont aa) alpontjába ütköző és aszerint minősülő, különösen nagy értékre elkövetett pénzmosás bűntett elkövetésével. A bűncselekmény elkövetése során betöltött szerepe szerint a bitcoint tartalmazó pénztárcákat összevonta, majd ezt követően X.Y., Z.Zs., valamint K.K. utasításainak megfelelően minden alkalommal a meghatározott mennyiségű bitcoint elkülönített pénztárcákba helyezte át annak érdekében, hogy azok kriptovaluta-konvertálással foglalkozó gazdálkodó szolgáltatásainak igénybevételével forintra átváltásra kerüljenek. Közreműködése a technikai részletek lebonyolítására irányult, továbbá ismerte az ehhez szükséges valamennyi privát és publikus kulcsot, amelyek a bitcoint tartalmazó pénztárca beazonosíthatóságához és az azokhoz tartozó utalások kezdeményezéséhez voltak szükségesek. Tevékenysége eredményeképpen 70 millió Ft értékű kriptovaluta átváltása volt sikeres, mindezek révén közreműködött az összegek végfelhasználói és a pénzösszegek eredete közötti egyértelmű összefüggés leplezésében.

A témaválasztás okai

A Készenléti Rendőrség Nemzeti Nyomozó Iroda Vagyon-visszaszerzési Hivatala (KR NNI VVH) két, 2018-ban megtartott magánlakásra irányuló kutatás során olyan eszközöket és adathordozókat foglalt le, amelyek alapján tizenegy fajta kriptodevizára történt vagyoni kényszerintézkedés, több mint száz millió forintos nagyságrendben.

A rendelkezésre álló adatok alapján ezek a virtuális pénzek kábítószerrel összefüggésbe hozható bűncselekményekből származtak, azonban más bűncselekményekből származó jövedelmek tisztára mosásának vagy elrejtésének is kiváló eszközei lehettek.

Feltételezem, hogy egy tanulmány ritkán kezdődik így, mint ahogy az a fentiekben olvasható. A kriptovaluták világa sem mindennapi rutinként

szerepel a bűnüldöző szervek tevékenységében, így egy kicsit rendhagyó módon mutatom be a címben megjelenő kérdéskör kezdeti fázisát.

Célom, hogy rövid betekintést adjak – jelen esetben – a BTC büntetőeljárásban történő megjelenésétől annak vagyonelkobzás céljából történő lefoglalásáig.

Szemléltetni fogom a nyomozás felderítési szakában végzett eljárási cselekményeket és azok eredményeit, illetve bemutatom a vizsgálati szakban felmerült sikereket és nehézségeket is.

A feldolgozandó tárgykörben nem az elméleti kérdések és fogalmak bemutatása lesz előtérben, annak tudását ugyanis feltételezem. Arra építve jelenítem meg a bemutatandó területet. Így nem is a már szakirodalomban megjelentek elemzésére és reflektálására vállalkozom, hanem a gyakorlati lehetőségeket ábrázolom.

A teljes, mindenre kiterjedő büntetőeljárás bemutatásától eltekintek, kimondottan csak a kriptovalutával összefüggésben felmerülő tevékenységet jelenítem meg.

A tanulmányban néhány problémát felvetek, amire a megoldás reményeim szerint a közeljövőben várható.

A büntetőeljárás szakaszai (felderítés, vizsgálat)

A felderítési cselekmények

A kiindulási adatok figyelembevételével a pénzmosás felderítésére irányuló eljárás feladata annak tisztázása volt, hogy a kábítószer-kereskedelem során keletkezett vagyont az elkövetők – annak bűnös eredetének ismeretében – pénzügyi műveletek révén hogyan használják fel, hasznosítják, és ennek során annak eredetét milyen módon leplezik.

Mindez óriási elemző munkát igényelt, külföldi társhatóságok bevonása is szükségessé vált. Így szereztünk tudomást arról a tényről, hogy a már említett darknetes piactér feletti rendelkezési jogosultságot az egyik európai nyomozóhatóság megszerezte, ezáltal hozzájutott valamennyi felhasználónévhez és jelszóhoz, illetve több ezernyi vásárló postázási címe vált hozzáférhetővé.

A külföldi nyomozószerv megküldte a „Csillag" nevű felhasználóval kapcsolatos jelentését, amely szerint nevezett 2016-ban regisztrált, utoljára pedig 2017 nyarán jelentkezett be. A jelentés szerint az 1m2m3n21v1c[1] bitcoin címet (address) használta, amely a bitcoin hálózat „főkönyvén" nyilvánosan hozzáférhető, úgynevezett blokkláncon[2] megtekinthető, illetve az oda küldött majd onnan továbbított bitcoin tranzakciók a cél, illetve forrás címekkel együtt beazonosíthatóak. Az elkövető az r6hne7x3y8h[3] visszatérítési bitcoin címet használta, továbbá az 1c51qbhmn[4] BTC címet is feltüntette, amely az információk szerint „Csillaghoz" köthető, és az Electrum[5] nevű alkalmazás használatával hozta létre.

A címek mellett ismert lett a felhasználó több jelszava is, illetve a jelentésből az is kiderült, hogy hozzá MDMA termékek árusítása köthető.

A nyomozás adatai alapján az említett bitcoin címeken valósult meg a BTC „tárolása". Minden címhez tartozott egy privát kulcs (private key)[6], amelynek ismerete a címen található BTC elköltéséhez volt számukra elengedhetetlen. Ez a kulcs gyakorlatilag megfejthetetlen, azonban a privát kulcs ismeretében megállapítható a bitcoin cím.

Az elemzett blokkláncon bitcoin címek és tranzakciók voltak láthatók. A rendszer névtelenségét egyébként az adja, hogy az egyes BTC címek – amelyekre leginkább bankszámlaszámként tekinthetünk – tulajdonosainak, azaz a privát kulcsot ismerő személy kiléte csupán a blokklánc által tárolt adatok ismeretében nem állapítható meg. Mindemellett arra lehetőség van, hogy más forrásból a bitcoin cím tulajdonosa megismerhető legyen.[7]

[1] A megjelenített bitcoin cím fiktív.
[2] Halász Viktor: A bitcoin működése és lefoglalása a büntetőeljárásban. Belügyi Szemle 2018/7–8. szám. 118. o.
[3] A megjelenített bitcoin cím fiktív.
[4] A megjelenített bitcoin cím fiktív.
[5] Asztali számítógépre letöltött, kétlépcsős azonosítással működő tárca.
[6] Metzger Máté: Módszertani útmutató. Virtuális fizetőeszközök. Nemzeti Szakértő és Kutató Központ. Budapest, 2020. 7. o.
[7] Metzger Máté (2020): i.m. 10. o.

A rendszer tehát nem teljesen névtelen, ezért vált ismertté a kábítószer-kereskedelemmel foglalkozó „Csillag" nevű felhasználó egyik bitcoin címe is.

Az address-eket – és a hozzájuk tartozó privát kulcsokat – kezelő alkalmazások általában nem egy, hanem több BTC címet is kezelnek egy tárcában (wallet)[8], amelyek egyetlen személyhez/személyi körhöz tartoznak. Egyetlen bitcoin cím ismerete általában nem elegendő ahhoz, hogy a hozzá tartozó privát kulcs ismerőjének valamennyi további, BTC pénztárcában található bitcoin címét megismerhessük, azonban bizonyos esetekben van mód kettő vagy több cím között ilyen kapcsolat megállapítására.[9]

Az egyes címek kapcsolatainak feltárásához az address-eket a blokklánc vizsgálatával tártuk fel – meghatározott módszerrel – egy weboldalon elérhető eszköz használatával. A program azonosította a megegyező BTC wallethez tartozó címeket, elemezte, hogy azok egy adott tranzakciónál szerepeltek-e forrás (input) oldalon, illetve más tranzakciók esetében mely más címekkel együtt fordultak elő az input oldalon együttesen. A bitcoin pénztárca azonosítását követően az eszköz egyedi azonosítóval látta el azt.

Az elemzések alapján láthatóvá vált, hogy a „Csillaghoz" tartozó, a külföldi nyomozóhatóság által megadott cím kétséget kizáróan igazolható, és a bitcoin útját tartalmazó címre egyenes úton is tranzaktáló cím azonos wallethez tartozik, azaz a kezelőjük azonos személy, ami egyértelműen bizonyítható a már fentiekben is említett blokklánc alapján.

Mindemellett azonban nemcsak a „számlatulajdonos" lett ismert a nyomozóhatóság előtt, hanem a blokklánc nyomon követésével a bitcoin további sorsa is kirajzolódott. Egyértelműen dokumentálhatóak voltak mind a BTC utalások, mind a forintra történő átváltások és készpénzfelvételek, majd a forintösszegek további számlák közti mozgását, illetőleg egyéb, vagyonkimentésként értékelt felhasználását is sikerült feltérképezni.

Az eddigiekben bemutatott elemzésen túlmenően megállapítható, hogy az a személy, aki a bitcoint a saját címére fogadja – tekintettel arra, hogy a

[8] Halász Viktor (2018): i.m. 123. o.
[9] Metzger Máté (2020): i.m. 11. o.

saját címét ismeri –, tisztában lesz a küldő címmel is a blokklánc nyilvánosságából fakadóan. Így bármilyen – a blokklánc megtekintésére alkalmas – eszközzel ellenőrizhető, hogy az 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 bitcoin címet is ismerni fog.

Ugyanez a gondolatmenet a bitcoint fogadó személyre is fennáll, azaz a fogadó – amennyiben előtte ismert a küldő személye – pontosan tudni fogja a forrás címről, hogy az kihez tartozik.

A nyomozóhatóságok részére a fentiek azt jelentik, hogy amennyiben sikerül beazonosítani egy adott bűncselekményhez köthető bitcoin címet, 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.

A nyomozás előre haladtával egy újabb szereplő lépett be:

S.S. szintén megalapozottan gyanúsítható pénzmosás bűntettének elkövetésével, mivel a rendelkezésre álló információk alapján tudomással bírt arról, hogy X.Y. és Z.Zs. kábítószer-kereskedelemmel foglalkoztak, amelyből bitcoinban és egyéb kriptovalutában nagy mennyiségű illegális jövedelemre tettek szert. Z.Zs.-vel házastársi kapcsolatban volt, amelyet Z.Zs. bűnözői tevékenységére tekintettel szándékosan bontottak fel, azonban S.S. tevékenyen közreműködött a bűncselekményből származó pénzösszegek eredetének leplezésében. Ennek keretében férjével közös széfszámlát üzemeltetett az egyik szomszédos országban, a Z.Zs. által a börtönből küldött levelek alapján kriptovalutákra intézkedéseket tett, a már bemutatott elkövetők által S.S. részére 150 000 eurót adtak át készpénzben és átutalás útján. Az illegális jövedelmet különböző hazai vagyonelemek vásárlására fordította, úgymint nagy értékű gépjárművek és ingatlanok, melyeken több tízmillió forintos átalakítást, felújítást végzett. Gyerektartás címén egy év leforgása alatt 50 millió forinttal gazdagodott.

Kriptovaluta konvertálása

Felmerülhet a kérdés, hogy mégis milyen módon tudja valaki a kriptovalutáját pénzre váltani és vice versa. Alapvetően – hasonlóan a hagyományos devizaváltásokhoz – magánszemélynél kialkudott árfolyamon, erre irányuló tevékenységet végző gazdasági társaságnál meghatározott árfolyamon, illetve kriptodeviza 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.[10]

A bitcoin váltással foglalkozó gazdasági társaságok, valamint a kriptodeviza tőzsdék általában egy weboldalon keresztül működtetik szolgáltatásaikat. Ezek a cégek a gyakorlati tapasztalatok alapján a tranzakciókat megelőzően általában megkövetelnek egy ügyfél-azonosítást, amely során a felhasználó személyazonosító okmányainak másolatait szerzik meg. Mindemellett más, az ügyfélhez köthető adatok is rendelkezésre állhatnak, így a weboldal elérésekor használt IP-cím, e-mail cím.

Megemlítendőek még az úgynevezett bitcoin ATM-ek, amelyek szintén BTC váltásra alkalmas készülékek. Ezek az eszközök készpénz kiadására és esetenként annak befogadására is alkalmasak. Készpénz kiadása esetén a felhasználó a saját bitcoin pénztárcájáról a cég BTC pénztárcájára utalja a felvenni kívánt deviza bitcoinban kifejezett ellenértékét, valamint megadja a mobilszámát (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.[11]

[10] Forrás: http://alapjogokert.hu/2020/04/14/a-blokklanc-technologia-es-a-kriptovalutak-mukodesenek-vizsgalata/
Letöltés ideje: 2020.04.14.

[11] Forrás: https://mfor.hu/cikkek/befektetes/a-kriptovaluta-valtas-es-vasarlas-kulisszatitkai.html
Letöltés ideje: 2019.01.10.

Hazánkban a legnagyobb kriptodeviza váltók a CoinCash Ltd., illetve a MrCoin.eu. 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).[12]

Kényszerintézkedések

„A bitcoin feletti rendelkezési jogot kizárólag a tulajdonossal szemben közvetlenül alkalmazott kényszerintézkedéssel, mégpedig egy kikényszerített tranzakcióval lehet felfüggeszteni, amely során a lefoglalandó bitcoint a tulajdonos címéről a hatóság címére utaljuk."[13]

A büntetőeljárásról szóló 2017. évi XC törvény (továbbiakban Be.) kialakította a virtuális vagyontárgyak biztosításának keretszabályait, amely alapján a virtuális fizetőeszközök lefoglalása végrehajtható oly módon, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adat által kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.[14,15] Ez praktikusan annyit jelent, hogy amennyiben virtuális valuta – 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 kriptovaluta címre utalják át, hogy az érintett személy semmiképp ne rendelkezhessen a lefoglalás tárgyával.

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

[12] Forrás: https://c□inmarketcap.c□m/rankings/exchanges/rep□rted/;
Mezei Kitti: A kriptovaluták kihívásai a büntető anyagi és eljárási jogban. Pro Futuro 2019/1. szám. 81. o.
[13] Halász Viktor (2018): i.m. 128. o.
[14] A büntetőeljárásról szóló 2017. évi XC. törvény 315. § (2) bekezdés
[15] Metzger Máté (2020): i.m. 24. o.

vagy az azt tartalmazó információs rendszer vagy adathordozó lefoglalásával kell végrehajtani.[16]

Speciális szabályként említhető, hogy 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.[17]

Tekintettel arra, hogy a Be. szerinti[18], a bűnjel és a bűnügyi vagyon kezeléséért felelős szerv még nem működik, valamint a 11/2003 (V. 8.) IM-BM-PM együttes rendelet alapján a lefoglalt elektronikus adatot adathordozón vagy a hatóság rendelkezése alatt álló tárhelyen kell őrizni[19], azonban ez a szabályozás csak 2021. január 1-jétől hatályos, a lefoglalás időpontjában, 2018-ban a megfelelő jogszabályi környezet hiányával álltunk szemben.

A fentiekben vázolt jogi környezet korántsem könnyítette meg a nyomozószerv munkáját, hiszen a vagyoni kényszerintézkedés időpontjáig Magyarországon és az európai országok túlnyomó többségében bitcoin lefoglalása nem történt.

A nyomozás folytatása mellett ki kellett dolgozni egy olyan módszertant, amely megfelel a büntetőeljárásról szóló törvényben foglaltaknak, a kriminalisztika szabályainak és a vonatkozó rendeleteknek is. Mindez az ügyészség és a bíróság támogatása nélkül nem valósulhatott volna meg.

Ennek eredményeként a KR NNI Vagyon-visszaszerzési Hivatal létrehozta az első hatósági pénztárcákat, melyekkel lehetővé vált a virtuális valuták lefoglalása.[20]

[16] 11/2003 (V. 8.) IM-BM-PM rendelet 67. § (5) bekezdés
[17] 11/2003 (V. 8.) IM-BM-PM rendelet 67/A. § (4) bekezdés
[18] Be. 36. § (2) bekezdés
[19] 20/2020. (XII. 30.) IM rendelet 33. § alapján
[20] Halász Viktor (2018): i.m. 129. o.

A hosszú ideig tartó felkészülést követően a kutatás során[21] az elektronikai eszközök, adathordozók vizsgálata volt az egyik legfontosabb tényező, valamint a papír alapú feljegyzések áttekintése sem maradhatott el, mivel többek között bitcoin pénztárca, a pénztárcát helyreállító kód (recovery seed) vagy BTC váltásra utaló böngészési előzmény feltalálását is valószínűsítettük.

Szoftveres pénztárcák

A szoftveres pénztárcák olyan számítógépes vagy mobiltelefonos alkalmazások, amelyek többnyire egy grafikus felületen keresztül kommunikálnak a felhasználóval, és lehetővé teszik a kriptodeviza egyenleg, a címek, a tranzakciók megtekintését, illetve kriptodeviza küldését vagy fogadását. A leggyakrabban használt ilyen alkalmazás Bitcoin esetében az Electrum nevű program.

Több olyan alkalmazás is létezik, amely nem csak bitcoin, de akár más kriptodevizák privát kulcsainak tárolására is alkalmas. Ilyen például a JAXX vagy a képeken feltüntetett egyéb alkalmazások.[22]

1. számú kép: Egyéb bitcoin alkalmazások ikonjai;
2. számú kép: JAXX alkalmazás ikonja

[21] Be. 302. §

[22] Metzger Máté (2020): i.m. 11. o.; Mezei Kitti (2019): 81.

Hardveres pénztárcák

A szoftveres 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 kriptodevizák privát kulcsait, akár egyidejűleg többfélét is. Ezek az eszközök PIN kóddal védettek, ezért hozzáférni – a kód ismeretének hiányában – csak a tulajdonos együttműködésével lehetséges.

3. számú kép: Hardveres pénztárcák

Az ilyen pénztárcák esetén egy számítógépes szoftver is szükséges a küldéshez, fogadáshoz. Az egyetlen – és egyben a biztonság szempontjából nagyon fontos – funkció, hogy a tranzakció jóváhagyását magán az eszközön egy gombnyomással vagy PIN kód beírásával kell végrehajtani.[23]

Recovery seed (helyreállító kulcs)

A helyreállító kulcs vagy recovery seed az úgynevezett determinisztikus pénztárcák esetén bír jelentőséggel.[24]

[23] Metzger Máté (2020): i.m. 12. o.
[24] Mezei Kitti (2019): i.m. 80. o.

Mind a hardveres pénztárcák[25], mind a legtöbb szoftveres pénztárca[26] 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.

Mindez úgy lehetséges, hogy a szavak által megtestesített kódból egy matematikai eljárással generálják a privát kulcsokat és a címeket, amelyek hozzáférést biztosítanak az összegekhez.

4. számú kép: Hardveres pénztárca és az ahhoz tartozó helyreállító kulcs

[25] USB porton, számítógéphez csatlakoztatható eszközök, amelyek titkosítottan tárolják a virtuális valuták privát kulcsait, akár egyidejűleg többfélét is. Ezek az eszközök PIN kóddal védettek, ezért hozzáférni – a kód ismeretének hiányában – csak a tulajdonos együttműködésével lehet.

[26] Olyan számítógépes vagy mobiltelefonos alkalmazások, amelyek többnyire egy grafikus felületen keresztül kommunikálnak a felhasználóval, és lehetővé teszik a kriptovaluta egyenleg, a címek, a tranzakciók megtekintését, illetve azok küldését vagy fogadását. A Bitcoin Core alkalmazást, amely eredetileg a legelterjedtebb volt, már kevesebben használják, mivel a működéséhez a teljes blokklánc letöltése szükséges, így akár több napig is tarthat, mire a valaha volt összes bitcoin tranzakció letöltésre kerül.

Eljárásunk során ilyen feljegyzések segítségével sikerült valamennyi virtuális valutát lefoglalni. Erre nemcsak a helyszínen, kutatáson adódott lehetőség, hanem a lefoglalt helyreállító kulcsok vizsgálatával, amely a kutatást követő napokban történt. Több recovery seed-en szerepelt feljegyzés arról, hogy melyik alkalmazással kell használni.

Ezekben az esetekben az adott szoftverbe a szavak beírása megtörtént, és így a pénztárcák generálása is sikeres volt.

A bitcoinon kívül több kriptovaluta jelenlétével szembesültünk, azonban a fellelt tucatnyi helyreállító kulcsnak tűnő feljegyzés között előfordult olyan 12 szavas lista, melynek a tetején az iOS alkalmazásokat a használó feljegyezte. Így a 12 szóval a pénztárca helyreállítása megtörtént, majd az összegek átutalása is lehetségessé vált.

Mindezeken felül a kutatást olyan időpontban kellett végrehajtani, amikor a célszemély számítógépe – nagy valószínűséggel – bekapcsolt állapotban van, hogy az ott tárolt adatokhoz együttműködő magatartás hiányában is hozzájuthassunk. A cél ebben az esetben a privát kulcs megszerzése és a tranzakció végrehajtása volt a hatóság által kezelt pénztárcába.[27]

Nyomtatott pénztárcák

Lehetőség van a privát kulcs papír alapú kinyomtatására is, amelyhez több alkalmazás is biztosít eszközt.[28] Ezen a privát kulcs titkosítás nélkül látható, ezért azt megmutatni senkinek nem szabad. Hatóságként a cél a privát kulcs megismerése, és a paper wallet-en található összeg hatósági pénztárcába történő küldése.

[27] Metzger Máté (2020): i.m. 25. o.
[28] bitadress.org

5. számú kép: Bitcoin pénztárca papír alapú kinyomtatott formában (paper wallet)

A képen látható paper wallet esetében a Spend felirat mellett látható az elköltéshez szükséges privát kulcs, a Load & Verify felirat mellett pedig a fogadáshoz szükséges publikus kulcs.[29]

Vizsgálati szak

A vagyoni kényszerintézkedéseket követő gyanúsítotti felelősségre vonások nem sok eredményt mutattak. Az eljárás alá vontak vallomást nem tettek, egyes kérdésekre válaszol(gat)tak, azonban a bizonyítékok felkutatása teljes egészében megtörtént.

Az eljárás indításakor nevesített 800 millió Ft-os vagyon az akkori bitcoin árfolyamot figyelembevételével alakult, azonban az érintett időpontban az kb. 160 BTC-nak felelt meg. A nyomozásban elvont kriptovaluták lefoglaláskori értéke nagyságrendileg 260 millió Ft-ot tett ki, ami azzal magyarázható, hogy 2018 januárja óta a bitcoin árfolyama jelentősen

[29] Metzger Máté (2020): i.m. 16. o.

lecsökkent. Az elkövetőket ez a tényező is motiválhatta abban, hogy a virtuális valutában tárolt vagyont forintra váltsák, illetve azt vagyontárgyakba fektessék.

Az árfolyamban 2021 első negyedévére számottevő változás állt be, a tanulmány írásakor online források alapján[30] 1 BTC megközelítőleg 58 616 USD értékkel bír. Valamennyi kriptovalutában tárolt vagyon értéke jelenleg vélhetően meghaladja a kb. 1,9 milliárd(!) forintot.

Jövőbeli lehetőségek

Napjainkban a már említett Be. 315. § (2) bekezdése alapján fizetésre használt elektronikus adat (virtuális fizetőeszközök) lefoglalásának kérdése egyre gyakrabban felmerül.

A fent hivatkozott szakasz, mely szerint *„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”*, feltételezi, hogy a lefoglalással érintett személy rendelkezik a virtuális fizetőeszközzel.

Az ilyen eszközök fő tulajdonsága, hogy központi szervezet nélkül, decentralizáltan működnek, a felettük való rendelkezést egy karaktersorozat, a privát kulcs testesíti meg. Aki a privát kulcsot ismeri, az rendelkezik a virtuális fizetőeszközzel.

Amennyiben a privát kulcs egy kutatás során az érintett személynél található meg, az azt jelenti, hogy ő mindenképpen rendelkezik az adott kulcs mögött megtestesülő virtuális fizetőeszközzel, így a lefoglalás a fellelt privát kulcs felhasználásával egyszerűen végrehajtható a hatóság kezelésében álló címre történő átutalással.

Számos esetben azonban a virtuális fizetőeszközök felhasználói nem ismerik a privát kulcsaikat, azaz közvetlenül nem rendelkeznek a felmerülő

[30] Forrás: www.napiarfolyam.hu/arfolyam/bitcoin
Letöltés ideje: 2021.05.09.

virtuális fizetőeszközökkel, hanem azokat a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról szóló 2017. évi LIII. törvény (PMT)[31] szerinti, vagy annak megfelelő külföldi virtuális és törvényes fizetőeszközök, illetve virtuális fizetőeszközök közötti átváltási szolgáltatásokat nyújtó szolgáltatónál, illetve letétkezelő pénztárca-szolgáltatónál tartják. Ez azt jelenti, hogy az említett szolgáltató tartja nyilván, hogy az általa kezelt virtuális fizetőeszközök közül a felhasználó mekkora összeggel rendelkezik, és a felhasználó megbízása alapján hajt végre tranzakciókat az összeggel (ugyanúgy, mint ahogy egy bank is kezeli az ügyfelei pénzét).

Ebben a helyzetben tehát az érintett személytől a tulajdonát képező virtuális fizetőeszköz lefoglalása nem lehetséges, mivel az a privát kulcsokkal nem rendelkezik (tehát magával a fizetőeszközzel nem ő rendelkezik). Természetesen a szolgáltató megkeresése minden további nélkül lehetséges, aki a lefoglalásban közreműködhet, a tranzakció a hatóság virtuális fizetőeszköz tárcájába végrehajtható lesz.

Abban az esetben azonban, amikor a szolgáltató külföldi joghatóság alá tartozik, a megkeresése gyakran csak hosszadalmas jogsegélyeljárás során lehetséges, ami alatt a gyanúsított vagy más hozzá kapcsolódó személy a felhasználói fiókba beléphet, és a virtuális fizetőeszköz átutalására megbízást adhat. Különösen akkor súlyos ez a probléma, ha az érintett szolgáltató olyan joghatóság alá tartozik, amellyel a kölcsönös jogsegélyre vonatkozó megállapodások hiányában csak nagyon hosszú idő alatt vagy egyáltalán nem lehet a vagyon biztosítása érdekében történő kapcsolatfelvételre lépéseket tenni.

A vázolt helyzetben is technikailag, viszonylag egyszerűen – feltéve, hogy a belépéshez szükséges adatok rendelkezésre állnak – végrehajtható lenne a vagyonelkobzás alá eső virtuális fizetőeszköz elvonása oly módon, hogy a nyomozóhatóság a kutatás során az érintett személynek a szolgáltatónál vezetett felhasználói fiókjába webes felületen belép, majd ott a szolgáltatónak megbízást ad, hogy a hatósági virtuális fizetőeszköz címre az

[31] 2017. évi LIII. törvény 1. § (1) bekezdés n)

érintett vagyonelemeit tranzaktálja át. Mindez teljesen automatikus rendszereken zajlik, technikailag ugyanaz történik, mintha egy külföldi pénzintézet netbankjába történne meg a belépés, és az ott található összeg átutalását követően a rendőrség letéti számlájára érkezik.

Amint látható, ez a módszer bár gyors és egyszerű, de az ügyfél nevében egy külföldi virtuális fizetőeszköz váltónak tranzakciós megbízást adni nem felel meg a hatályos eljárási normáknak.

Felmerül a kérdés: vajon lehetséges-e a külföldi virtuális és törvényes fizetőeszközök, illetve virtuális fizetőeszközök közötti átváltási szolgáltatásokat nyújtó gazdálkodó internetes felületére a tulajdonos nevében belépve megbízást adni a szolgáltatónak, hogy a hatóság kezelésében álló címre küldje meg a vagyonelkobzás végrehajtásának biztosítása céljából lefoglalandó virtuális fizetőeszközt, amennyiben az megfelelően dokumentált, és az alkalmazandó kényszerintézkedés más módon történő végrehajtása kizárható?

Továbbá: lehetséges-e illegálisan működő szolgáltatók (váltók, piacterek) felületére belépni, és onnan a lefoglalás végrehajtása érdekében a vagyonelkobzás alá eső vagyont képező virtuális fizetőeszközt átutalni a hatóság címére a megfelelő dokumentáltság mellett, amennyiben a beszerzett adatok alapján e szolgáltató hatósággal történő együttműködésének lehetősége kizárható?

Álláspontom szerint ezeknek a kérdéseknek a megválaszolása jogszabály-módosítást is generálhat.

A mai világban a bűnözés is rohamosan fejlődik. Új módszerek jelennek meg mind a bűncselekmények elkövetésében, mind a legális úton szerzett vagyon elrejtésében, ezért elengedhetetlen, hogy a bűnüldöző szervek felkészülten álljanak a kihívások elé, és mindezekre az igazságszolgáltatás is megfelelő mértékben reagáljon.