

SIMON BÉLA

Kriptovaluták – rendészeti válaszok¹

Az optimális rendészeti fellépés érdekében szükséges, hogy legyenek ismereteink a kriptovalutákkal összefüggő jogsértések jelenlegi és prognosztizálható volumenéről.

Az árfolyam meredek emelkedésének az egyik legnagyobb korlátja, hogy a kriptovalutákban nem teljes a bizalom. Időről időre bekövetkeztek olyan tényezők, amelyek megrengették a felhasználók bizalmát. Ezek egy része teljesen független a kriptovalutát fenntartó informatikai hálózattól, de arra jelentős hatással bíró teljesen legális döntés. Ilyenek voltak, amikor számos ország vagy multinacionális vállalkozás elzárkózott a kriptovaluták elfogadásától, vagy betiltotta.

Nem zárható ki azonban, hogy egy-egy kriptovaluta hanyatlásához nem ártó szándékú, hanem helytelen belső piaci döntések vezetnek. Az egyes kriptovaluták nem változatlanul működnek megalkotásuk óta. A bitcoint – mint a legjelentősebb kriptovalutát – fenntartó szoftvernek tizenhat fő továbbfejlesztett verziója készült el 2018 júniusáig. A bitcoin üzemeltetése felett hatalmat gyakorló szervezetek döntésén múlt az is, hogy 2017. augusztus 1-jén az addig önállóan fejlődő bitcoinblokklánc kettéágazott, és kivált belőle a bitcoin cash². Ez a döntés nem ingatta meg a bitcoinba vetett bizalmat, de nem kizárható, hogy a későbbiekben az egyes kriptovaluták kibocsátói, fejlesztői helytelen döntéseikkel viszik hanyatlásba az egyes kriptovalutákat, vagy olyan új kriptovaluták jönnek, amelyek letaszítják a jelenleg értékes digitális pénzeket.

Az egyes kriptovaluták – és a bennük felhalmozott érték – tehát ártó szándék nélkül is könnyen elszenvedhetnek hatalmas árfolyamvesztéseket, elértéktelenedést.

A kriptovaluták árfolyamát nagyon jelentősen visszavető illegális tevékenységek is jelentkeztek a múltban. Volt példa arra, hogy bitcoin kereskedelmével

¹ A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, *A jó kormányzást megalapozó közszolgálat-fejlesztés* elnevezésű kiemelt projekt keretében működtetett Concha Győző Doktori Program keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.

² A bitcoin utalási költségeinek és időigényének emelkedése miatt a kis összegű, nagy számú tranzakciók gyors végrehajtását célzó technológiai változtatással egy új kriptovalutát hoztak létre. Akinek az elágazás előtt volt bitcoinja, az ez után ugyanannyi bitcoin casht is kapott a tárcájába.

foglalkozó tőzsde üzemeltetői a kezelésükre bízott bitcoinnal sajátjukként rendelkeztek, és eltérő adatokat mutattak az ügyfeleknek, mint amekkora az összeg valójában volt. Volt arra is példa, hogy egy jelentős forgalmú tőzsde informatikai rendszerét támadás érte, és megsemmisültek a tárcaadatok.

Tekintsük át, hogy összességében milyen illegális folyamatok, cselekedetek vezethetnek a felhasználók, tulajdonosok sérelméhez!

A blokklánc-technológiából adódó veszélyek

A kriptovaluták belső működéséből, a blokklánc-technológiából eredő veszély elméletileg elenyésző.

A blokklánc-technológia – különösen a bitcoin esetében – a matematikai algoritmus, a számítógépes program következtében védve van a visszaélések ellen. A privát kulcs „kitalálásának” esélye a program oldaláról szinte zéró³. A kriptovaluták értékét éppen az adja, hogy a tudomány mai állása szerint szinte hamisíthatatlanok, feltörhetetlenek. A blokklánc hamisításához olyan számítási kapacitásra volna szükség, amely erősebb a jelenleg a rendszerben működő összes csomópont teljes számítási kapacitásánál⁴. A technológiából származó sérülékenységek azonban léteznek. Tekintettel arra, hogy ezek a visszaélések olyan szintű informatikai ismereteket igényelnek, amely meghaladja e tanulmány jellegét és kereteit, ezért bemutatásukra csak példálózva és érintőlegesen kerül sor.

Kétszeres elköltés

Visszaélésre ad lehetőséget – jellemzően a bitcoin esetében –, ha valaki a blokklánc véglegessé válása előtt egy újabb transzferálást végez. Mivel az egyes blokkokat a feldolgozó számítógépek nem feltétlenül a beküldés sorrendjében dolgozzák fel, ezért lehetséges, hogy az elkövető egy személyes találkozón a kriptovalutáért kapott pénz átvételekor a telefonján vagy a laptopján elindítja az utalást, majd néhány percen belül átutalja a teljes számlaegyenlegét egy másik tárcára úgy, hogy a kéréseket feldolgozó és a blokkláncot generáló számítógépek számára (mivel erre van lehetőség) na-

³ Bár a kvantumszámítógépek fejlesztésével lehetséges, hogy például egy RSA algoritmussal kódolt adat is rövid időn belül feltörhető lesz.

⁴ Ez az úgynevezett 51 százalékos támadás, ami egyéb hackertechnikával (a rendszer két részre szakításával) akár 33 százalékos számítási kapacitással is lehetséges.

gyobb összegű felajánlást tesz a blokkba foglalásra és véglegesítésre. Ekkor előfordulhat, hogy a korábban kezdeményezett utalás nem teljesül a tárca üressége miatt.

A decentralizált autonóm szervezet

A bitcoin utáni legnagyobb kapitalizációval bíró altcoin az ethereum, amely egy világméretű decentralizált hálózat létrehozatalán túl lehetőséget teremtett az úgynevezett okosszerződések megkötésére, amikor a tranzakciók valamilyen feltétel bekövetkezésétől teljesülnek⁵. Az ethereumban lehetőség van ICO-k (*Initial Coin Offering*) kibocsátására, ami egy-egy kriptográfiával megtámogatott közösségi finanszírozási modell. Egy ilyen ICO a decentralizált autonóm szervezet (*Decentralized Autonomous Organization; DAO*), ami arra gyűjtött támogatásokat, hogy az abban részt vevők a közvetlen demokrácia eszközével dönthettek, támogatnak-e, vagy sem egy projekteket, és döntéseiknek megfelelően részesülnek a sikerből.

Amiért a decentralizált autonóm szervezet fontos témánk szempontjából, az az, hogy 2017 júliusában az összeggyűjtött 170 millió amerikai dollár értékű ethereum kriptopénzből (ether) 53 millió amerikai dollár⁶ értékben utalt magának egy személy az algoritmus hibáját kihasználva. A vélemények még abban is eltérnek az eset kapcsán, hogy mennyiben volt szabálytalan/jogellenes az utalás, hiszen nincsenek előírások ezeknek a tranzakcióknak a szabályos lebonyolítására. A tranzakciót megvalósító személy az algoritmusban rögzített feltételek szerint cselekedett, azaz utalta saját részére a kriptovalutákat, így bár az alkotók szándékával ellentétes volt a transzferálás, de nem volt szabályrendszer, amelyet sérteni kellett a művelethez.

A konszenzus elleni támadások

Ezeknél az a lényeg, hogy a blokkláncot létrehozó számítógépek közti megállapodásban érnek el olyan tranzakciókat, amelyek rendes működés mellett nem következnenek be. Szükséges hozzá a rendszerben működő eszközök felletti irányítási jog, vagy a kriptográfia feltörése, de mindkettőnek rendkívül kicsi az esélye.

⁵ <https://www.ethereum.org/>

⁶ David Siegel: Understanding The DAO Attack. Coindesk.com, Jun 25, 2016. <https://www.coindesk.com/understanding-dao-hack-journalists/>

Sybil-támadás

Sybil-támadásnál a támadó előállít egy szimulált P2P bothálózatot, amivel megpróbálja a decentralizált konszenzust befolyásolni, azaz a blokkláncot fenntartó számítógépeknek azt a látszatot kelti, hogy az általa irányított hálózat a teljes blokkláncot tartalmazó teljes csomópont, pedig valójában nem.

Maginot-vonal-támadás

E támadási forma nem a számítási kapacitással kapcsolatos, hanem a lekötött kriptovaluta összegétől függ. Ha az összes lekötött összeg 51 százalékát leköti az elkövető, akkor lehetősége van az összeget kétszer elkölteni, ezáltal összeomlasztani a kriptovalutát. Ez a kriptovalutát fenntartó informatikai rendszer működéséből adódik. A lényege, hogy hatalmas összeget kellene arra fordítani, hogy megvalósulhasson, és az eredménye az volna, hogy a kriptovaluta teljesen elértéktelenedik, így megvalósulásának esélye elenyésző.

DDoS-támadás

A blokklánc fenntartásáért felelős hálózati eszközök, számítógépek elosztott túlterheléses támadásával akadályozható a rendszer, de szétagoltsága miatt nem következhetnek be nagy károk, inkább csak a szolgáltatás ideiglenes lassulása⁷.

Az előbbieken túlmenően is léteznek elméletben támadási metódusok a blokklánc-technológia ellen, de azok megvalósításának esélyei szintén csekélyek.

Az informatikai eszközökből származó veszély⁸

E körbe sorolhatjuk azokat az elkövetési magatartásokat, amikor nem a blokklánc-technológia esetleges sérüléseit kihasználva, hanem a kriptovalu-

⁷ Trinh Anh Tuan – Szegő Dániel: Ezek a legvadabb módszerek, amelyekkel kifosztják a bitcoinosokat. Portfolio.hu, 2018. április 24. <https://www.portfolio.hu/vallalatok/it/ezek-a-legvadabb-modszerek-amelyekkel-kifosztjak-a-bitcoinosokat.282664.html>

⁸ Természetesen a blokklánc-technológiát működtető hálózat elemei is informatikai eszközök, de a könnyebb megértés érdekében célszerű különválasztani az üzemeltetői oldalt (blokklánc-technológia működtetői) és a felhasználói oldalt (kriptovaluta-tulajdonosok).

ták megszerzésének, tárolásának, transzferálásának folyamata során használt informatikai eszközöket éri támadás.

Ezek a támadások jellemzően olyan sérülékenységeket, kompromittálási lehetőségeket használnak ki, amelyek a kriptovalutáktól függetlenül is léteznek.

Ebben az esetben célszerű az egész folyamatot végigtekintenünk, és kiemelni a gyenge pontokat.

Az átlagos felhasználó a kriptovalutára nem bányászat útján⁹ tesz szert, hanem valamilyen formában vásárolja. A vásárláshoz egy tárca alkalmazást használ. A nem megbízható forrásból telepített tárca alkalmazások önmagukban tarthatnak olyan kódokat, amelyek arra szolgálnak, hogy a manipulált tárca alkalmazás által tárolt kriptovaluták felett az elkövetők átvegyék az irányítást.

Ha az alkalmazás megbízható forrásból származik, és a privát és publikus kulcs generálása is szabályosan – egyedi és befolyástól mentes formában – megtörténik, akkor a felhasználó ezt a sérülékeny pontot átlépte. Ha azonban a kulcsok generálását valamilyen nem megbízható forrásra bízta, akkor a beszerzett kulcspárt az elkövetők bármikor felhasználhatják, amikor azt látják a blokkláncon, hogy azon jelentősebb értékű kriptovaluta jelent meg. Például ha egy erre kifejlesztett oldalon az elkövetők naplózzák a magmondatok segítségével, vagy bármilyen módon generált kulcspárokat, akkor nincs más teendőjük, mint folyamatosan ellenőrizni, hogy megjelennek-e a publikus kulcsok a blokkláncon¹⁰.

De a generált kulcspárok bármilyen informatikai eszközön bármelyik létezési formájukban elméletileg megszerezhetők: a vágólapra másolt kódsorokat, a papír tárcaként kinyomtatni szándékozott fájlokat a nyomtatóra küldés előtt, vagy a nyomtatót kompromittálva lehetőség nyílik az ártó szándékú beavatkozásra.

Kriptovalutákat érintő kártékony kódoként detektáltak olyan – az operációs rendszer sérülékenységét kihasználó malware-t, amely a háttérben futva folyamatosan figyeli, hogy mikor helyez a felhasználó vágólapra egy publikus kulcsot, majd amikor a beillesztésre kerül sor, akkor a sértett már az elkövetők által meghatározott kódsort – azaz saját publikus kulcsukat – illesz-

9 Nagy számítási kapacitású számítógépek, vagy célhardverek (berendezésorientált áramkör, Application-specific integrated circuit; ASIC) használatával megvalósított eljárás, amelynek eredménye, hogy a blokkláncon megjelenik a bányászatot végző számára bizonyos mennyiségű kriptovaluta.

10 Legálisan is működnek olyan szolgáltatások, amelyek e-mailt küldenek a regisztrált személynek, ha az általa követni szándékolt publikus kulcs megjelenik a blokkláncon.

ti be. Mivel a kódsorok nehezen megjegyezhetők és könnyen összekeverhetők, ezért a sértett már csak a teljesített utalás után észleli, hogy kriptovalutáját nem szándékolt tárcába utalta.

A szolgáltatók igénybevételeivel használt online tárcák esetében azok az információs rendszereket érő visszaélési formák lehetségesek, amelyek például az internetes bankolásnál megvalósulhatnak.

A különbség azonban nagyon lényeges: egy internetes bankolás során megvalósuló visszaélésnél az illegálisan utalt összeget vissza lehet származtatni, a készpénzfelvételt meg lehet akadályozni, és még a pénzügyi intézet is kártalaníthatja a sértettet. A kriptovaluták világában azonban ez nem így van. Az átvitel nem visszavonható, jellemzően nem kapcsolható konkrét személyhez, és a szolgáltatók tipikusan nem vállalnak kötelezettséget a kártalanításra.

Bár a kriptovaluták tárolására a hardveres tárcákat tartják az egyik leginkább megbízható formának, mégis előfordulhat ezek sérülékenysége, még ha ennek esélye meglehetősen kicsi is¹¹.

Az informatikai eszközök kompromittálásával megvalósuló visszaélések között említhető a korábbi terminológia szerinti „gépidőlopáshoz”¹² hasonló elkövetés, amelyben az elkövetők különféle kártékony kódokkal, *script*ekkel arra bírják rá a sértett informatikai eszközeit, hogy azok kriptovalutákat bányásszanak¹³. A tevékenység nem a kriptovaluta-tulajdonosokat sérti ugyan, és nem okoz jelentős kárt, de büntető törvénykönyvünkbe ütköző.

Természetesen nem csak ügyfél oldalon vannak kitéve az értékek a kibebűnözőknek. Több esetben előfordult, hogy az ügyfeleknek forró tárcát, vagy tőzsdei kriptovaluta-szolgáltatást nyújtó szolgáltatók informatikai rendszereit kompromittálták az elkövetők, és megsemmisítették a tárcaadatokat, vagy maguknak átvitelték azok állományát.

Utóbbi visszaélésekre az ad lehetőséget, hogy a szolgáltatóknak nincsenek olyan nemzetközi szabványaik, mint például a bankkártya-üzletágban megszokott előírások¹⁴.

11 Andriana Gkaniatsou: Bitcoin hardware wallet vulnerability exposes funds to hackers: study. https://www.ed.ac.uk/files/atoms/files/bitcoin_wallet_devices_vulnerable_to_security_hacks_study_shows_23.01.2018.pdf

12 Szathmáry Zoltán: Bűnözés az információs társadalomban. Alkotmányos büntetőjogi dilemmák az információs társadalomban. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2012, 100. o.; Nagy Zoltán: Az informatika és a büntetőjog. Magyar Jog, 1991/1., 21–26. o.; Nagy Zoltán: A számítógéppel megvalósítható vagyoni jogsértésekről. Bűnügyi Műhelytanulmányok, 1992/1., 22–26. o.

13 <https://news.bitcoin.com/hackers-target-400000-computers-with-mining-malware/>

14 PCI DSS bővebben lásd https://www.pcisecuritystandards.org/pai_security/

Tehát a kriptovalutával megvalósított ügyleteknél használt informatikai eszközök (telefonok, asztali számítógépek, laptopok, szerverek, okosórák, pendrive-ok) esetén nagyon fontos azok integritásának megléte¹⁵.

E visszaélések megelőzésére az információbiztonsági tudatosság fejlesztése a leghatékonyabb eszköz. A bekövetkezett visszaélések felderítésére a kimagaslóan képzett nyomozó hatósági munkatársak és a piaci szereplőkkel való szoros együttműködés ad lehetőséget.

Kriptovaluta a bűnös vagyon tárolására és a pénzmosás

Ebben az esetben a konkrét cél jellemzően nem a kriptovaluta megszerzése, hanem a más elkövetésből származó illegális bevételeket az elkövetők kriptovalutába fektetik, majd a későbbiek folyamán saját céljaikra, vagy más jog-sértő cselekmények (például terrorizmus) finanszírozására fordítják¹⁶.

Ily módon a bűnelkövető nagy valószínűséggel elvonhatja a hatóságok intézkedései előtt a megszerzett illegális javakat, ezáltal csökkenti a nyomozás eredményességét, megghiúsítja a vagyon elvonását, a sértettek polgári jogi igényének kielégítését.

A pénzmosás már a bitcoinnal kapcsolatos legkorábbi tanulmányok során is felvetődött kockázati tényezőként¹⁷, és azóta is az egyik legtöbbször emlegetett veszélyforrásnak tekinthető a kriptovaluták és a kriminalitás kapcsolata-t vizsgáló értekezésekben¹⁸. Mindennek egyik legfőbb oka, hogy az utóbbi huszonöt évben a pénzmosás elleni közös nemzetközi fellépés fő irányvona-la az volt, hogy a pénzügyi közvetítő szolgáltatókat ügyfél-azonosítási és gyanús pénzmozgások bejelentésére irányuló kötelezettségekkel terheltek, a kriptovaluták a decentralizáltságukkal pedig elegánsan kiléptek az e szabá-lyok hatóköre alól.¹⁹ Véltetően jó részben ez is az oka annak, hogy amikor egy-egy jogalkotó rászánja magát manapság kriptovalutákkal kapcsolatos normák megalkotására, ezt mindenekelőtt a pénzmosás elleni küzdelem je-

¹⁵ Muha Lajos: A kritikus információs infrastruktúrák védelme. Reinet Technológia Kft., Budapest, 2015

¹⁶ Természetesen itt elmosódik a határ azokkal a bűncselekményekkel, amelyek esetében eleve a bitcoin megszerzése a cél.

¹⁷ Lásd például Reuben Grinberg: Bitcoin: An Innovative Alternate Digital Currency. In: Hastings Science & Technology Law Journal, vol. 4, no. 1, 2011, p. 204.

¹⁸ Gyarakai Réka: Az ördög pénze? A Bitcoin. Detektor Plusz, 2016/23., 1–3. o.
<http://detektorplusz.hu/index.php?m=23458>

¹⁹ Robert Stokes: Anti-money laundering regulation and emerging payment technologies. In: Banking & Financial Services Policy Report, vol. 32, no. 5, 2013, p. 3.

gyében teszi²⁰ (mint ahogy láthattuk ezt az európai pénzmosás elleni irányelv legutóbbi módosítása kapcsán is)²¹.

A pénzmosással kapcsolatos vádak vonatkozásában a kriptovalutákkal összefüggésben az azokat támogató személyek érvei között is megjelenik, hogy a készpénz sokkal inkább alkalmas e tevékenység folytatására, de könnyű rejtethetősége, gyors és olcsó transzferálása a kriptovalutákat könnyebben alkalmazhatóvá teszi e célra.

A kriptovalutákat pénzmosásra nemcsak anonimitásuk okán érdemes az elkövetőknek használniuk, hanem amiatt is hogy egyre több helyen lehet közvetlenül ellenszolgáltatást teljesíteni általuk²².

Az ellenőrző/felügyeleti rendszer hiányából adódó veszély

A pénz- és tőkepiacok ártalmas befolyásolásának korlátozására számos jogintézmény kialakítására került sor az elmúlt évszázadokban. Az egyik legfontosabb, hogy a résztvevők körének jellemzően egy szűrésen kell átesnie²³. A kriptovaluták esetében nem működik ilyen módon a belépési korlát. Jelentős online jelenléttel és marketinggel a hozzáértés szinte pótolható. A másik jelentős veszélyforrás, hogy nincsen jegybanki rendszer és intézkedési lehetőség az árfolyamok befolyásolására. A hatalmas árfolyammozgások akár csalárd szándékkal is előidézhetők, de a rendszer normális működéséből is következhetnek²⁴. A kriptovaluták jogi szabályozása nem megoldott. Nem alakult ki egységes jogalkalmazói gyakorlat az esetlegesen fellépő jogviták orvoslására.

20 Ne tévesszen meg senkit, hogy a pénzmosás esetén a magyar szabályozás következetesen bűncselekményből származó *dologgal* kapcsolatos cselekményekről rendelkezik. A dolog fogalma itt nem a Ptk.-ban használatos dologfogalommal egyenértékű, hanem a szabályozás az alapját képező, 1990. november 8-án, Strasbourgban aláírt nemzetközi egyezményben szereplő dologfogalmat emelte át. Ez magában foglalja a megfogható és megfoghatatlan dolgokat egyaránt, és a kihirdetésről szóló 2000. évi CI. törvénnyel a magyar jogrendszer részévé is vált. Belovics Ervin – Molnár Gábor Miklós – Sinku Pál: Büntetőjog II. Különös rész. HVG-ORAC, Budapest 2013, 738–739. o.

21 Halász Viktor: Kriptovaluták a bűnüldözésben. Új kihívások és lehetséges válaszok. Diplomamunka. Nemzeti Közszerológiai Egyetem Nemzetközi és Európai Tanulmányok Kar, Budapest, 2018, 40. o.

22 <https://coinmap.org>

23 Például értékpapírok tőzsdére bekerülése, vagy kereskedelmi bank alapítása számos feltétel teljesítése után lehetséges.

24 A 317 amerikai dollárról 0,1 amerikai dollárra esés a piaci működés következtében. <https://blog.gdax.com/eth-usd-trading-update-5d8142b5bdc1>

A büntető törvénykönyv számos tényállást tartalmaz, ami a gazdaság jogszerű működését hivatott védelmezni:

- belépési küszöb védelmére hivatott a jogosulatlan pénzügyi tevékenység²⁵ bűncselekményének pönalizálása²⁶;
- a bennfentes kereskedelem büntette²⁷, bennfentes információ jogosulatlan közzétételének vétsége²⁸, illetve tiltott piacbefolyásolás büntettét²⁹ elkövetnék mindazon személyek, akik álhírekkel, publikációkkal, egy-egy kriptovaluta dömping jellegű felvásárlásával, értékesítésével olyan módon befolyásolják az árfolyamot, amely tisztességtelen és jellemzően a többi befektető kárából jogtalanul maga vagy a megbízottja tesz szert vagyoni előnyre.

E tényállások azonban csak akkor vehetők figyelembe, ha a kriptovaluták pénzügyi eszközöknek minősülnének. Sem a befektetési vállalkozásokról és az árutőzsdei szolgáltatókról, valamint az általuk végezhető tevékenységek szabályairól szóló törvény³⁰, sem a tőkepiacról szóló törvény³¹, sem a Magyar Nemzeti Bank pénzügyi eszközök jegyzéke³² nem minősíti a kriptovalutákat pénzügyi eszközöknek.

Ha azonban a kriptovaluta kibocsátója gazdálkodó szervezet és valaki e gazdálkodó szervezet vagyoni helyzetéről vagy vezető állású személyéről e tevékenységével összefüggésben valótlan adat közlésével vagy híresztelésével, illetve adat elhallgatásával másokat tőkebefektetésre vagy a befektetés emelésére, illetve tőkebefektetés eladására vagy a befektetés csökkentésére rábír – akkor a magatartása tényállásszerű lehet a kriptovalutákra vonatkozóan is, és elkövetheti a tiltott piacbefolyásolás büntettét³³.

25 A büntető törvénykönyvről szóló 2012. évi C. törvény 408. §.

26 A hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény szerinti pénzügyi szolgáltatási vagy kiegészítő pénzügyi szolgáltatási tevékenység körében értékelhető sok olyan tevékenység, amely a kriptovaluták váltásával, kereskedelmével foglalkozik.

27 Btk. 410. §

28 Btk. 410/A §

29 Btk. 411. §

30 2007. évi CXXXVIII. törvény

31 2001. évi CXX. törvény

32 <https://www.mnb.hu/felugyelet/szabalyozas/mifid-mifir/penzugyi-eszkozok-jegyzeke/penzugyi-eszkozok-jegyzeke-2018/penzugyi-eszkozok-jegyzeke-2018-marcius>

33 Bár e tényállás az elmúlt öt évben a Belügyminisztérium Bűnügyi Statisztikai Rendszere szerint egyszer sem valósult meg, így nehezen elképzelhető, hogy a kriptovalutákkal összefüggésben a regisztrált bűncselekmények közt megjelenne.

A kiberbűncselekményekkel foglalkozó sajtó az elmúlt évben gyakorta tudósított az ICO-kkal³⁴ mint startup vállalkozásokkal kapcsolatos visszaélésekről.

A Magyar Nemzeti Bank tájékoztatása szerint „*Akár befektetett tőkéjük egy részét vagy egészét is elveszthetik azok az ügyfelek, akik tokeneket vásárolnak nyilvános ICO forrásgyűjtés keretében tőkebevonásra, cégfejlesztésre hivatkozó személyektől. Az MNB és az Európai Értékpapír-piaci Hatóság is folyamatosan figyelmeztet – az egyre inkább terjedő – befektetés jelentős kockázataira.*”³⁵ Az ICO-k jelentős kockázatot hordoznak magukban, tekintettel arra, hogy a legtöbbször csak egy ötlet létezik, és semmilyen megvalósítási feltétel nem adott, a befektetők pedig könnyelműen bíznak a projekt sikerében mindenféle ellenőrzés nélkül. Emiatt az ICO-kibocsátások nagy része pénzügyileg bukás a befektetők számára³⁶.

Sok esetben előfordult, hogy a befektetések összeomlásakor a befektetők hiszékenységet kihasználva és az adott kibocsátó munkatársának kiadva magukat, az elkövetők arra kérték a károsultakat, hogy további regisztrációs díj, vagy a tárca azonosítása céljából küldjenek kisebb összegű kriptovalutát – jellemzően ethert. Ezáltal az egyébként is károsult személyeket további vagyonelemről fosztották meg.

A visszaélések megakadályozása érdekében szükséges volna megelőzés-ként széles körű tájékoztatást végezni azon célcsoportok körében, amelyek vélhetően kriptovalutákkal összefüggő üzleti befektetéseket hajtanak végre. Az elmúlt időszak – de leginkább a bitcoin 2017-es szárnyalása – vélhetően Magyarországon is sok olyan embert csábított kriptovaluta vásárlására, akinek a rendszer működésével összefüggésben nincs széles körű tapasztalata. Fontos, hogy az ezzel kapcsolatos konferenciákon, internetes fórumokon jelenjenek meg magyar nyelven is azok az információk, amelyek gyanút ébresztenek például egy-egy rendkívül csábító ICO-val összefüggésben.

Kriptovaluták mint a bűnelkövetés segédeszközei

A kriptovaluták és leginkább a bitcoin egyik legnagyobb visszhangot kiváltó megjelenési formája a darknetes kereskedelemben történő felhasználás. A Silk-

³⁴ Ezekről információt az icodrops.com oldalról is lehet gyűjteni.

³⁵ <https://www.mnb.hu/sajtoszoba/sajtokozlomenyek/2017-evi-sajtokozlomenyek/rendkivuli-kockazatot-hordoznak-az-ico-befekteteseik>

³⁶ Horváth Ferenc: A kriptovalutákkal történő visszaélések. Szakdolgozat. Nemzeti Közsolgálati Egyetem Rendészettudományi Kar, Budapest, 2018, 16. o.

Road nevű platform 2013-as felszámolásakor megállapították, hogy az illegális áruk és szolgáltatások óriási volumenű kereskedelme zajlott, és az ellenérték kiegyenlítésére szinte kizárólag bitcoint használtak. Kriptovaluták hiányában a darknetes kereskedelem semmiképp nem fejlődhetett volna ilyen szintre.

Az elmúlt időszakban számos hasonló szolgáltatás indult a torhálózat³⁷ által fenntartott internetes felületen. Ezekkel összefüggésben számos olyan eredményes nemzetközi nyomozás fejeződött be, amelyekben a hatóságoknak sikerült az ügyletekben részt vevők széles körét beazonosítaniuk és eljárás alá vonniuk.

Az ilyen jellegű bűncselekményekkel szemben szoros nemzetközi együttműködés, a titkosszolgálati eszközök összehangolt alkalmazása és a legjobb gyakorlatok megosztása vezethet eredményre. Ezek részletes bemutatása azonban nem része e tanulmánynak.

Csalás jellegű veszélyek

Amint említettem, a kriptovalutákkal összefüggésben jelentős online jelenlét, keresőoptimalizálással, micro-targeting³⁸ módszerekkel elérhető, hogy a célcsoport folyamatosan olyan hirdetésekkel találkozzon, amelyek látszólag valamilyen kiváló üzleti lehetőségről szólnak, de valójában hólabda-³⁹ csalások, piramisjátékok⁴⁰, vagy egyszerű csalások.

Az elkövetők számos csalási metódust alkalmaznak, amelyek a blokklánc-technológiával kapcsolatos kifejezések használatával hihetővé teszik a sértettek számára a tettes által közvetítetteket.

Például:

- kriptovaluta közös bányászatára vonatkozó felhívás a kezdeti költségek megelőlegezésével valós bányászati kapacitás nélkül;

³⁷ <https://www.torproject.org/>

³⁸ <https://policyreview.info/articles/news/political-micro-targeting-hijacking-european-democracy/753>

³⁹ E csalástípusnál a sértettektől jelentős hozam ígéretével gyűjtenek az elkövetők pénzt befektetésre, miközben valós gazdasági lehetőségeik nem adnak alapot a hozam garantálására. Az esetleg kivett összegekre a kezdeti időszakban a többi sértett betétjéből történik hozamkifizetés. Kellően nagy összegű betét összegyűjtése után az elkövetők azzal sajátjukként rendelkeznek.

⁴⁰ A rendszer működéséhez szükséges, hogy az abba belépők vagyoni hozzájárulást teljesítsenek a rendszerbe, majd újabb személyeket vonjanak be, akik szintén vagyoni hozzájárulást teljesítenek, és beszerveznek további személyeket. A több szintű marketing (Multi Level Marketing) rendszertől az különbözteti meg, hogy piramisjáték esetében a beszervezettek a befizetett összegért nem kapnak értékkel bíró dolgot.

- szinten már működő kriptovaluta-bányászati kapacitás lekötése garantált nyereséggel a kezdetben befizetett költségek megfizetése után⁴¹;
- az elkövető az általa fejlesztett speciális (titokzatos) algoritmus által prognosztizálni tudja a kriptovaluták árfolyammozgását, és garantálja a rendkívül magas hozamot (szintén hólabdacsalás). Erre jó példa a BitConnect esete, amikor egy valós blokklánc-technológiához egy piramisjátékot szerveztek azt ígérve, hogy egy speciális kereskedőalgoritmus segítségével a cég a betett összegek után több ezer százalékos éves hozamot képes elérni, amihez az is szükséges, hogy a befektetők meghatározott ideig ne vegyék ki betéteiket, és további betéteseket szervezzenek be⁴²;
- valamilyen véleményformáló, vagy gazdag személynek kiadva magát az elkövető arról ad tájékoztatást, hogy mindenkinek küld jelentős mennyiségű kriptovalutát, de a transzferáláshoz szüksége van a sértettek publikus kulcsára, ezért teljesítsenek egy kis értékű kriptovaluta-utalást az elkövető által megjelölt tárcába;
- scamcoinok – csalás jellegű kriptovaluták esetében az elkövetők létrehoznak egy altcoin – egy új kriptovalutát –, majd annak jelentős részét kibányásszák. Ez után megfelelő marketingeszközök használata mellett elkezdnek a saját tárcáik között egyre magasabb árfolyamon kereskedni a kriptovalutával. Ha megfelelően sok külső befektető is vásárol az egyébként értéktelen kriptovalutából, akkor az elkövetők kiszállnak az illegális profittal⁴³;
- „nigériai levél” jellegű csalások, amikor is e-mailben, vagy más formában arra bírják rá a sértettet, hogy a diktátor mesés vagyonának utalásához, vagy az afrikai szépség kiszabadításához, vagy hatalmas nyeremény, örökség utalásához a szükséges „csekély” értékű kriptovalutát transzferálják az elkövető tárcájába;
- működnek olyan vállalkozások is, amelyek a kriptovaluta látszatát keltve betétet gyűjtenek, és jelentős hozam ígérete mellett buzdítják a betéteseket újabb betétek fizetésére és további személyek bevonására. Ennek ellenértéként az elkövetők által kifejlesztett „kriptovalutát” kapják. Valójában a

41 A sértetteknek nem tűnik fel, hogy vajon miért adja át kriptovaluta bányászati kapacitását a felajánló negyven amerikai dollár értékben, ha magának is bányászhatna ez idő alatt százdollárnyi értékűt. Ha azonban megbízható vállalkozás a kapacitása bővítésére gyűjt pénzt, akkor az üzleti megoldás lehet legális és rentábilis is.

42 Az elkövetésben keveredett a hólabda csalás, (amikor csak irreálisan nagy hozamot ígért a befektetőknek valós gazdasági tevékenység nélkül), illetve a piramisjáték szervezése (amikor a várt jutalmat/eredményt más személyek beszerzése, betéte által lehet elérni).

43 Hasonlít a tiltott piacbefolyásolásra, de ebben az esetben az egész altcoin létrehozása a csalást szolgálja.

kibocsátott saját „kriptovalutának” nincs valós értéke, valódi pénzre való átváltása nem lehetséges, és nem a blokklánc-technológiától, hanem csak a kibocsátótól függ, mennyi van belőle⁴⁴;

- lehetséges olyan pénzügyi szolgáltatás csalárd indítása is, amelyben az „ál-szolgáltató” azt a látszatot kelti, hogy az ügyfelei által részére utalt valódi pénzből az ügyfelek számára forró tárcát tart fenn – azaz az ügyfél csak a publikus kulcsát látja webes felületen, vagy csak a számlaegyenleget –, majd amikor kellő számú betét gyűlt össze, akkor a virtuálisan létező és egyébként üres tárcákat magukra hagyják, és az ügyfelek befizetéseit sajátjukként használják az elkövetők;
- mint említettem, a kriptovaluták kapcsán ugyanolyan elkövetési magatartások lehetségesek, mint az internetes bankolásnál. A forró tárcák esetében is előfordulhat, hogy az elkövetők e-mailben kérik a sértettet arra, hogy a küldött linken keresztül a publikus kulcs mellett adja meg jelszavát is az azonosításhoz⁴⁵;
- lehetséges a csalás elkövetése offline is. Az elkövetők internetes fórumon eladásra kínálnak nagyon kedvező áron kriptovalutát, amelyet személyes találkozó keretében kívánnak értékesíteni. A találkozón az elkövetők a pénz sértettől történő átvétele után látszólag az ügyletben szereplő kriptovalutát transzferálják, majd elhagyják a helyszínt. Az ügylet tárgya azonban soha nem érkezik meg a vevőhöz. Hasonló módon valósulhat meg lopás vagy akár rablás is.

A csalás jellegű bűncselekmények esetében több esetben előfordult, hogy a tettes – felkészülve a csalásból származó javakra – az elkövetés előtt bitcoinvásárlást kezdeményez valamely online kriptovaluta-váltónál, majd a váltó által – általában e-mailben – megküldött bankszámlaszámot a vásárlás azonosításához szükséges közleménnyel úgy küldi tovább a sértettnek, mintha az a sajátja lenne (kéri természetesen a közlemény feltüntetését is). Az összeg beérkezése után a váltó abban a hitben van, hogy a fizetést az elkövető végezte, így a bitcoint elutalja a tettes által megadott címre. Ezek a szolgáltatások nagyban megnehezítik minden bűncselekmény felderítését, amikor is az elkövetők célja a haszon-szerzés. Ezzel összefüggésben számos tényállás felvetődhet a sorozatjellegű aukciós csalásoktól a terrorcselekményig. Az a különlegessége, hogy a pénzvál-

44 Például a OneCoin. Bővebben lásd www.onecoin.eu; <https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2017-evi-sajtokozlemenyek/a-onecoin-elleni-fellepesrol-targyalt-a-piacfelugyeleti-munkacsoport>

45 Ezekben az esetekben is a kétfaktoros azonosítás megakadályozhatja a visszaéléseket.

tók tevékenységének pillanatában a bűnös forrásból származó előny egy mozzanatban válik elérhetetlenné a sértett számára és válik a nyomozó hatóság számára nehezen elérhetővé. Mindez úgy valósul meg, hogy az alapügy elkövetője csak nagyon rövid ideig tevékeny az elkövetésben⁴⁶.

Mint látható, a csalás jellegű visszaélések közt nincs sok újdonság. Ugyanazok a sémák jelennek meg, de a kriptovalutákba vetett túlzott bizalom, és az a tény, hogy a kriptovaluták az eddig megszokott pénzüpiaci folyamatoktól jelentősen eltérnek⁴⁷, alkalmas a sértettek józan értékítéletének, kételkedésének legyőzésére.

E visszaélésekkel összefüggésben is a lehetséges sértettek tájékoztatása, a megtörtént visszaélések publikálása okozhatja a bűncselekmények számának visszaesését.

A megvalósított bűncselekményekkel összefüggésben a nyomozó hatóságok a blokkláncok elemzésével és a feltételezett elkövetők feltérképezésével, adatbázisok létrehozásával érhetnek el eredményeket, tekintettel arra, hogy e téren az elkövetői kör megfelelően kvalifikált kell hogy legyen, így lehetőség nyílik az egyes személyek kriminalizálódásának nyomon követésére⁴⁸.

Rendészeti válaszok

Azt nehéz megjósolni, mekkora erőforrást kell lekötni a rendészeti szerveknél a kriptovalutákkal kapcsolatos problémák orvoslására. Az azonban tény, hogy 2012 és 2017 között 141 büntetőügy kapcsolódott a kriptovalutákhoz, ami összességében nem sok, de a 2012-es egy büntetőügyhöz képest a 2017-es ötvennyolc ügy exponenciálisan emelkedő görbét mutat.

Vélhetően a következő években sem történnek a kriptovaluták kapcsán olyan bűncselekmények, amelyek érdemben befolyásolnák Magyarország gazdasági érdekét, hiszen nem nagy az ország veszélyeztetettsége. Az azonban valószínűsíthető, hogy sok sértettet érintő jogsértés kerül napvilágra. Ezen túlmenően annak is fontos szempontnak kell lennie, hogy az állampolgároknak a nyomozó hatóságokba vetett bizalmát és az eljáró szervek megbecsültségét nagyon pozitívan befolyásolná, ha az ilyen ügyeket szakértő módon, gyorsan és eredményesen fejeznék be a hatóságok.

⁴⁶ Egy váltásdíj átvétele, vagy az utalt pénz továbbutalása/felvétele, vagy a pénzmosási folyamat számos buktatót tartogat az elkövetők számára, itt azonban ezek egy mozzanatban javarészt megvalósulnak.

⁴⁷ Például hogy 2017 januárjától egy év alatt huszonegyszeresére nőtt az árfolyama.

⁴⁸ Fórumnyilatkozatokban, online jelenlétnél stb.

A leginkább akut probléma a bűnüldöző szervek számára a büntetőeljárásokban felvetődő kriptovaluták kezelése.

Abban minden szakértő egyetért, hogy az elkövető által használt és a saját tárcáját tartalmazó informatikai eszköz (számítógép, pendrive, telefon stb.) fizikai lefoglalása nem elegendő a kriptovaluta feletti felügyelet megszerzésére.

A kriptovalutákra vonatkozó vagyoni kényszerintézkedések módszertani utasítása jelenleg zajlik.

Az elkövető részéről tulajdonképpen elegendő akár a tárcát záró privát kulcs ahhoz, hogy a kriptovaluták feletti felügyelet ő, vagy a megbízottja megőrizze oly módon, hogy azt transzferálja egy általa létrehozott és a hatóság által nem ismert tárcába.

Éppen ezért a hatóság részéről is elsődleges feladat a kényszerintézkedéssel érintett tárca tartalmának lefoglalásaként egy a hatóság felügyelete alatt álló tárcába transzferálása. Ez a tranzakció azonban összetett hatósági intézkedés esetén nem kívánt módon információt szolgáltat az elkövetőtársaknak, hiszen ők a blokkláncból rájöhetnek erre.

A hatósági tárcába történő átutalás azonban számos további problémát vet fel.

Az egyik ilyen a hatósági tárca kompromittálása⁴⁹. Erre jó válasz lehet a több jelszóval védett (*multisig*) tárca és a hardvertárca.

A másik nehézség az elvont kriptovaluták tárolása, kezelése, értékesítése. Megítélesem szerint a lefoglalást szenvedőt nyilatkoztatni kell arra vonatkozóan, hogy kívánja-e a kriptovaluta értékesítését. Ennek célja annak elkerülése, hogy a terhelt felmentése és a kriptovaluta neki való visszaszolgáltatása esetén kár érje az eljárás időtartama alatti esetleges árfolyamcsökkenéssel. Ha az értékesítés mellett dönt a lefoglalás szenvedője, akkor az új büntetőeljárási törvényben van egy újítás előzetes az értékesítésre vonatkozóan, miszerint az általános feltételtől eltérést engedve, az értékesítés egy opcionális esetét is bevezeti a 319. § (4) bekezdésben. Ha a lefoglalt dologgal kapcsolatban bejelentettek megalapozott igényt és az értékesítéshez a megalapozott igény bejelentője hozzájárult, a lefoglalt dolog értékesítése elrendelhető.

⁴⁹ A bitcoinnal kapcsolatos, eddigi legnagyobb sajtófigyelem mellett zajló büntetőügyben (Ross Ulbricht DPR, bővebben: Andy Greenberg: Silk road creator Ross Ulbricht loses his life sentence appeal. <https://www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-life-sentence-appeal/>) megtörtént, hogy szövetségi ügynökök lopták el a bűnös forrásból származó bitcoinokat. Bővebben lásd <https://www.wired.com/2016/11/ross-ulbrichts-lawyers-point-another-corrupt-agent-silk-road-case/>

Az elmúlt időszakban a kapcsolódó kutatások középpontjában sokkal inkább a technológia és a funkcionalitás állt, míg javarészt figyelmen kívül hagyták az értékteremtő tevékenységeket és az irányítás kérdését⁵⁰. Azt mindenképpen fontos leszögezni, hogy a blokklánc-technológia multidiszciplináris megközelítést követel.

E tanulmány célul tűzte ki, hogy megvizsgálja a kriptovaluták tekintetében fennálló jelenlegi problémákat, és becsléseket ad a rendészeti szervek szükséges intézkedéseire.

Operatív szinten szükséges a blokklánc-technológiához kapcsolódó ismeretek elmélyítése a bűnüldöző és titkosszolgálati szervek állományában.

Fontos kiaknázni a bűnüldözési célú nemzetközi együttműködésből származó lehetőségeket, megismerni a legjobb gyakorlatokat, esettanulmányokat, részletszabályozási megoldásokat, használni a közös erőforrásokat⁵¹.

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-nyilvántartás⁵² belföldi pénzintézetektől, 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 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, online-tárca-szolgáltatók, kriptopénz-ATM-üzemeltetők stb.), hogyha az ügy-

50 Marten Risius – Kai Spohrer: A Blockchain Research Framework. Business & Information Systems Engineering, vol. 59, no. 6, 2017, pp. 385–409. <https://doi.org/10.1007/s12599-017-0506-0>

51 Például az Europol EC3 blokklánc-elemző platformja.

52 Bár e cikk írásakor is vannak kedvező jelek arra, hogy ez megvalósul.

felét 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 nagyon jelentős részben a kapcsolódó jogi szabályok határozzák meg, azazhogy az egyes államok milyen mértékben tiltják, korlátozzák a használatukat.

Korábbi kutatási eredményekből jól látható, hogy a kriptovalutákat nagy arányban használják bűncselekmények elkövetéséhez⁵³, illetve bűnös forrásból származó javak mozgatására, elrejtésére. Megítélésem szerint bizonyosan maradnak olyan államok – jellemzően offshore területen –, amelyekben a kriptovaluták konvertibilis valutákra történő átváltása megoldható marad, így nem vonhatók ki a kriptovaluták a pénzmosás eszköztárából. Sokkal célszerűbb szélesebb körben lehetőséget adni nekik, és a saját jogrendszerünkben 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 torhálózatához: a szellemet nem lehet visszazárni a palackba, így meg kell próbálnunk kordában tartani és a lehetőségekhez mérten felügyelni.

⁵³ Sean Foley – Jonathan R. Karlsen – Tālis J. Putņins: Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies? 2018.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102645