

A KRIPTOVALUTÁK ÉS A KAPCSOLÓDÓ RENDÉSZETI KIHÍVÁSOK

1. Bevezetés

Az emberi társadalom számos funkciót, eljárást és intézményt fejlesztett ki a saját maga és tagjai védelmére. Kijelenthetjük, hogy ezek a megoldások mindig akkor hasznosak, ha a kialakításuk, fenntartásuk során felhasznált erőforrások kisebbek, mint a védendő társadalmi érték, melynek megóvására hivatottak.

A helyes döntést egy mérleg két serpenyőjét vizsgálva találjuk: az egyik oldalon a védekezés költsége, a másik oldalon pedig a veszélyeztetett érték található. Utóbbi serpenyő távolságát a felfüggesztéstől a kár bekövetkezésének valószínűsége határozza meg. A súlyok és arányok azonban nehezen meghatározhatók. Ebben az összefüggésben vizsgáltuk a kriptovaluták problémakörét. Mekkora érték? Mekkora veszély? Mekkora intézkedéseket kell tenni a lehetséges problémákra?

Vajon egy hirtelen felkapott téma a kriptovaluták okozta új problémák, és felesleges vele foglalkozni, vagy valóban forradalmasíthatja a pénzügyi rendszert és akár befolyásolhatja a társadalom működését?¹

A cél tehát a kriptovaluták közérthető bemutatásán keresztül kiemelni néhány aspektust, amelyre a rendészeti szerveknek választ kell adni.

2. Mi is a kriptovaluta?

Számos definícióval találkozhatunk e fogalom körül határolása során. Az alábbiakban megkíséreltem olyan kis mértékben informatikai szakkifejezéseket használva leírni a működést, ami a továbbiak megértéséhez feltétlenül szükséges.

Gyakran a kriptovalutákat és az elektronikus pénzt egymás szinonimájaként használják. A két fogalom azonban élesen elválik egymástól. Az elektronikus pénz a jegy-

¹ Korábban az internetről sem feltételezték, hogy ilyen átütő hatása lesz a mindennapjainkra, továbbá ha nem is megyünk vissza a távoli múltba, akkor a Facebook is egy jelentéktelen internetes oldallak tűnt sokak számára.

bankok által kibocsátott pénz egyik – dematerializált – megjelenési formája, de azzal azonosjoghatásokkal.² A kriptovaluták esetében azonban nem beszélhetünk jegybanki, vagy állami elfogadásról³ – azokat mindenki önként elfogadhatja olyan értéken, amennyiért akarja: csak a kereslet és kínálat határozza meg az árfolyamot, így a monetáris politika eszköztársa sem működhet. A kriptovalutákat – bár pénz funkcióval bírnak – nem nevezhetjük törvényes fizetőeszköznek, azaz pénznek.

Sok esetben a virtuális valutát és a kriptovalutákat egymás szinonimájaként használják. A virtuális valuta sokkal tágabb kör. A virtuális valuták digitális formában megjelenő, de állami szabályozás nélküli valuták⁴. A kriptovaluták ezen belül képeznek egy csoportot, amelyeknek az a sajátos ismérvük, hogy kriptográfiai hitelesítő folyamatok – tipikusan blokklánc technológia – által lehet őket létrehozni.

Fontos leszögezni, hogy a bitcoin⁵ csak egy a több ezer kriptovalutából, de vitathatatlanul a legnagyobb hatású. A sikerén felbuzdulva sok csoport írt számítógépes programot, amely kriptovaluták előállítását teszi lehetővé, és ezek közül vannak, amelyek szolgáltatásaikban, felhasználhatóságukban felülmúlják a bitcoint, de jelenleg ez a kriptovaluta a legelterjedtebb és ez rendelkezik a legnagyobb bizalommal a felhasználók részéről. A lényegesebb kriptovaluták különféle internetes oldalakon ismerhetők meg.⁶

1. táblázat: Pénz mátrix

A pénz mátrix ⁷			
Jogi státusza szerint	Szabályozatlan	egyes helyi valuták	Virtuális valuták
	Szabályozott	Bankjegyek és érmék	elektronikus pénz számlapénz (letét)
		fizikai	digitális
		megjelenési forma	

² A hitelintézetekről és a pénzügyi vállalkozásokról szóló 2013. évi CCXXXVII. törvény 6. § 16. pontjában megfogalmazottak szerint.

³ Az MNB már 2014. évben rendkívül kockázatosnak ítélte a bitcoint (300-1000 USD közti árfolyamsávban). https://www.mnb.hu/archivum/Felugyelet/root/fooldal/topmenu/sajto/sajtokozlomenyek/bitcoin_kozl [2018.04.30] Azonban vannak olyan törekvések, ahol önkormányzatok elfogadják, vagy a blokklánc technológiát állami célokra használják. <https://coincolors.co/2017/09/12/dubajban-lakast-svajcban-adot-lehet-fizetni-bitcoinnal/> [2018.04.30.]

⁴ Ide tartoznak különféle számítógépes játékokban gyűjthető „érmék” is még akkor is, ha azokat valamilyen formában rendes pénzre lehet váltani.

⁵ Szokásos rövidítése: BTC.

⁶ Ilyen például a <https://coinranking.com/> és a <https://coinmarketcap.com/>.

⁷ <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf> [2018.05.26.]

A témánk szempontjából leglényegesebb közös jellemzőik:

- központi adminisztráció/felügyelet nélküli rendszer
- alkalmas a pénz funkcióinak ellátására.

Nakamoto Satoshi⁸ feltaláló célja a 2007-08-as gazdasági válság időszakában az volt, hogy kialakítson egy decentralizált és önmagát fenntartó pénzügyi rendszert, amely sokkal hatékonyabb és olcsóbb, mint a jelenlegi bankrendszer. A megoldást egy olyan szisztéma kidolgozásában látta, amely nem a közvetítőbe helyezett bizalomra épít, hanem kriptográfiára és elemi számítások sokaságára bízva a tranzakciók validálását, egy peer-to-peer hálózaton. Ez mindaddig biztonságot nyújt az egész rendszernek, amíg a rendszert becsületesen használni kívánók összességé több számítási kapacitással bír, mint bármely a rendszer kijátszására apelláló személy vagy csoport a hálózatban.⁹

Ahhoz, hogy ez a rendszer kialakulhasson, először motiválni kell a lehetséges szereplőket, hogy belépjenek. Ezt a motivációt a bányászat által megtermelt kriptovaluta jelenti. Ha már egyszer kialakult, akkor akár a tranzakciós díjakból is fenn tartható a működés.

Ahhoz, hogy valami pénzként funkcionáljon – szükséges egy központi elem, amelyben a felek megbíznak. A bankrendszerben, a nemzeti valutákban ezt a bizalmat többek között:

- a pénzintézeteket szabályozó jogi normák,
- a kapcsolódó intézmények és
- az állami kezességvállalás tartják fenn.¹⁰

A kriptovaluták esetében a bizalom legfontosabb – és talán egyetlen – alapja az a matematikai algoritmus, amely az adott kriptovalutát létrehozta. Ez egy bonyolult egyenlet, melyhez összetett számítási folyamatokon keresztül véges számú megoldás társul. A bitcoin esetében ez közel 21 millió. Aki kriptovalutát bányászik, az a számítógépének teljesítményét az adott kriptovalutához kapcsolódó matematikai feladvány számítására áldozza.¹¹ Ennek ellentételezéseként időszakonként kriptova-

⁸ Ezen a néven kerültek publikálásra a bitcoin rendszer alapvetései, de máig nem ismert az a konkrét személy vagy csoport, aki ezt kidolgozta.

⁹ BAKÓ Tamás: Bitcoin hálózatok elemzése (Diplomamunka). Eötvös Loránd Tudományegyetem, Természettudományi Kar, Matematikai Intézet 2015. 7. o.

¹⁰ Bármelyik bizalmi alapként működő elem gyengülése a nemzeti valuta gyengülését is eredményezi.

¹¹ Az önálló bányászat nem jellemző. Gyakrabban csoportokba (pool) gyűjtik a bányász gépeket és a közös bitocint felosztják egymás közt a munkájuk arányában. Ilyen bányász pool-ok például a következők: F2Pool, KnCMinerB, AntPool, MaxBTC, BitFury/SEGWIT stb.

lutákat kap¹² a sok egymással mellérendelő viszonyban álló számítógépből felépülő nagy internetes hálózatból¹³.

Az, hogy bizonyos javakból korlátozott mennyiség áll rendelkezésre, az mindenképpen árfelhajtó hatású.¹⁴ A korlátozott számú előállíthatóság minden kriptovaluta esetében érvényes.

Ahhoz, hogy egy digitális jel önmagában értéket képviseljen, ahhoz meg kell szüntetni egyik legfontosabb tulajdonságát, azt, hogy a róla készült másolat vele teljesen azonos¹⁵. A kriptovaluták esetében ezt úgy oldják meg, hogy ezeket a digitális jeleket egymáshoz fűzik és egy nagy egyenrangú internetes hálózatban nagyon sok számítógép egymással párhuzamosan ugyanazon egymáshoz fűzött adatot fűzi tovább¹⁶. Ez a blokklánc. A blokklánc megmutatja, hogy ebben az adatfolyamban az „egyenlet melyik megoldása” melyik megfejtőnél van, vagy azt kinek adta tovább.

Nagyon fontos, hogy a kriptovaluták jellemzően feloszthatók. A bitcoin esetében ez nyolc tizedesig lehetséges 1 bitcoin = 100.000.000 satoshi. Tehát amint a forintnak a fillér (volt) a két tizedesig tartó váltópénze, úgy a bitcoinnak a satoshi a 8 tizedesig tartó váltópénze.

Az előbbi példánál maradva tehát ha valaki egy hagyományos számítógéppel elkezd bitcoint bányászni, akkor annak ellentételezéseként nem csak egész bitcoint kaphat, hanem ennek tört részét is. Vásárolni is lehet tört bitcoint is, sőt az jellemző.¹⁷

Az adott kriptovalutát életben tartó blokklánc tehát folyamatosan nagyszámú számítógépen elérhető az interneten, ami egy peer-to-peer (P2P) hálózat, ami egészen más, mint az ügyfél-szerver megoldás. A peer-to-peer olyan, mint egy pletykahálózat, ahol mindenki elmondja néhány embernek a híreket (új tranzakciókról és új blokkokról), és végül az üzenet mindenki számára elérhető lesz a hálózatban.

¹² A kriptovalutát sem úgy kell elképzelni, hogy az egy egyedi karakterlánc, vagy kódsor, hanem az egy nagy főkönyvben egy bejegyzés, hogy egyik, vagy másik felhasználónak van belőle 2, vagy 0,0012 darab.

¹³ Maga a matematikai feladvány és annak megoldása a kriptovaluták működésének megértéséhez nem is fontos. Sőt maga a feladvány sem fontos a témánk szempontjából és a kriptovaluta fejlesztőknél is inkább az volt az egyik legfontosabb cél, hogy az informatikai eszközökkel erőforrásigényesen lehessen csak megoldani, azaz ne lehessen egy egyszerű számítógéppel megtalálni az összes megoldást.

¹⁴ A fordítottja is igaz, hisz ha sikerülne ólomból aranyat előállítani, vagy könnyen lehetne tiszta gyémántkristályokat előállítani, akkor értékük hatalmasat zuhanna.

¹⁵ Ha egy szöveges fájlról, képről, számítógépes programról, bekódolt merevlemezeiről bitről bitre készítek egy másolatot, akkor azok teljesen ugyanolyanok lesznek.

¹⁶ A folyamatosan és párhuzamosan fűzött blokkláncban benne van, hogy melyik tárca mikor és mennyi kriptovalutát kapott és azt megtartotta, vagy tovább transferálta.

¹⁷ Bővebben: <https://bitinfocharts.com/bitcoin/explorer/> ahol az is látható, hogy milyen tranzakciók kerülnek egy blokkba, azok mennyi időnként jönnek létre.

Ez ellentétben áll a hagyományosan használt ügyfél-szerver hálózattal, ahol a főnök az alárendelteknek tájékoztatja a híreket, és a főnök egy központi referenciapont és potenciális veszélyforrás: sérülésével megszűnik az információáramlás.¹⁸

A kriptovaluták felhasználhatóságát Satoshi Nakamoto is leginkább a bankrendszer kiváltásában látta, mivel olcsóbban tud működni, mint a jelenlegi bankrendszer. Azt is látnunk kell azonban, hogy a rendszer működése is erőforrás igényes (informatikai eszközök fejlesztése és működtetése leginkább) és egy kriptovaluta egység előállítása is bizonyos egységű egyéb javak felhasználásával történik¹⁹. A kriptovaluták akkor tudnak költséghatékony alternatívái lenni a jelenlegi pénzügyi rendszernek, ha egy adott egységnyi pénz funkciót (pl: x érték transferálása két fél közt) sokkal kedvezőbb költségekkel tudnak megvalósítani.²⁰

A kriptovaluták ún. tárcákban helyezkednek el. Ezek a tárcák a blokkláncba fűzve szintén digitális adatok. A tárcák is teljesen egyedi azonosítóval rendelkeznek. A tárcában való elhelyezést nem úgy kell érteni, hogy egy kódsor megjelenik egy mappában és minél több kriptovalutánk van, annál nagyobb lesz az adott fájl. E tekintetben sokkal inkább hasonlít a rendszer a banki számlapénzre, vagy az érték-papírszámlákra: amikor a bankszámlánkról utalás történik, akkor nem adott sorszámmú bankjegyek indulnak el a célszámlára, hanem van egy egyenleg és a számlatulajdonos utasítja a számlavezetőjét, hogy számláját annyival terhelje, amennyivel a célzott számlán jóváírást teljesít.

A kriptovaluták esetében tehát ez a blokklánc egy főkönyv, melyben folyamatosan szerepelnek a létrejövő kriptovaluták és azoknak az aktuális helye és mozgása is nyomon követhető. 2018 júniusáig a teljes bitcoin blokklánc mérete (adatbázis indexekkel) meghaladta a 15 GB-ot és a tárolt tranzakciók száma a 320 milliót.²¹

¹⁸ <https://bitsonblocks.net/2015/09/01/a-gentle-introduction-to-bitcoin/> [2018.05.25.]

¹⁹ Hasonlóan a jelenlegi pénznekél nem csak a pénzjegynyomda egy bankjegyre eső előállítási költségét kell figyelembe venni, hanem az egy egységnyi pénznek a pénz funkció betöltéséhez szükséges összes költségét (pld: egy átutalásnál a bank épületének, informatikai infrastruktúrájának arra eső költségét).

²⁰ Itt ismételtelen figyelembe kell venni a kriptovaluta előállítási költségén felül a rendszer fenntartásának, üzemeltetésének költségét az x egységnyi értékre vonatkozóan. Persze ezt a képletet a megbízhatóság és a kényelmi funkciók erősen árnyalják.

²¹ <https://blockchain.info/hu/charts/n-transactions-total?timespan=all> [2018.06.01.] Bővebben: <https://blockchain.info/charts>; E könyvrészlet írásakor a bitcoin esetében ez a tiszta blokklánc 170Mb – <https://blockchain.info/charts/blocks-size> [2018.06.05.]

3. Mi a kriptovaluta tárcá?

Bűnüldözési szempontból tehát nagyon fontos, hogy a nyomozás érdekében, vagy akár csak a polgárjogi igény érvényre juttatása miatt szükséges lefoglalni a kriptovalutákat, vagyis leginkább átvenni a hatalmat az érintett mennyiségű kriptovaluta felett. Ehhez szükséges ismernünk ezen javaknak a fellelhetőségi helyét – azaz a tárcákat (wallet).

A bányászattal nem foglalkozó személy, aki szeretne kriptovalutát tulajdonolni – mindenképpen egy tárca alkalmazást kell, hogy használjon²² (telefonon, számítógépen, tableten stb., szinte bármilyen operációs rendszeren).

A tárca alkalmazás legfontosabb funkciói:

- létrehozza tulajdonképpen a tárcát, ami a lehetőséget biztosítja a blokklánc-hoz való kapcsolódásra,
- létrehoz a tárcában publikus kulcsokat (public key – amit a számlaszámhoz hasonlatosnak tekinthetünk) és azokhoz illő privát kulcsokat (private key – amit a számlához tartozó jelszóként értékelhetünk),
- kapcsolatot tud kiépíteni a kriptovaluta blokkláncát üzemeltető internetes hálózattal és annak üzenetet tud küldeni és onnan üzeneteket tud megjeleníteni a kezdeményezett tranzakciókról.²³

A kriptovaluta tárcánk nem tárolja a megvásárolt, vagy kibányászott bitcoinokat, csak a számlaszámot (ez a publikus kulcs) és egy jelszót (ez a privát kulcs). Ezen a kulcspárok esetében nagyon fontos, hogy tulajdonképpen egyediek.

A bitcoin-ban egy privát kulcs 256 bites szám,²⁴ amely többféleképpen is megjelenhet. Egy hexadecimális (azaz 16-os számrendszerben felírt) 256 bites számot 64 karakterben lehet leírni, mely karakterek tartományai 0-9 vagy A-F.²⁵ A privát kulcs tehát egy nagyon hosszú szám-és betűsor, melyből a tárca alkalmazás nyeri a felhatalmazást arra, hogy a kriptovaluták feletti rendelkezéseket végrehajtsa, azaz

²² Még a blokklánc üzemeltetésében és fejlesztésében részt vevő bányászattal foglalkozó számítógépeknek is a munkájuk gyümölcseként kapott kriptovalutát is tárcákban kell elhelyezni.

²³ Számos további funkció is kapcsolódhat a tárca applikációhoz. Például jelszavas védelem az egész tárcára, a kriptovalutákkal foglalkozó tőzsdék adatainak megjelenítése stb.

²⁴ Azaz 256 karakteren 0, vagy 1 – így 2 a 256. hatványon verziót vehet fel – ez meglehetősen nagy variációt ad: összesen: 115.792 duodecillió 089.237 undecillió 316.195 decillió 423.570 nonillió 985.008 oktillió 687.907 szeptillió 853.269 szextillió 984 kvintilliárd 665 kvintillió 640 kvadrilliárd 564 kvadrillió 039 trilliárd 457 trillió 584 billiárd 007 billió 913 milliárd 129 millió 639 ezer 936 lehetséges variáció, ha a 10es számrendszert használjuk.

²⁵ Például: 5JbvhsfA5JesmcVTGNrb3gkHGGv67hwY5hUws1Pmdj65jRM9nPF

például elküldje azokat egy másik tárcába. Fontos, hogy privát kulcsból egy matematikai művelettel kialakítható a publikus kulcs,²⁶ de ez irreverzibilis folyamat. A publikus kulcs jellemzően 33, vagy 34 karakter hosszú és alfanumerikus jegyekből áll.²⁷ Tipikusan 1-es, vagy 3-as számjeggyel kezdődik.²⁸ Tehát aki ismeri a privát kulcsot, kontrollálja a tárca tartalmát.

3.1. KRIPTOVALUTA TÁRCA TÍPUSOK

A kriptovalutákhoz kapcsolódó kulcspár tárolásának számos formája alakult ki. Nem szükséges, hogy ez egy digitális kódsor legyen, hanem akár papírlapra írva, vagy IT eszközök által könnyen feldolgozható módon (pld kinyomtatott QR kód) is tárolhatók, vagy akár meg is jegyezhetők (vagy egy memorizált dalszövegből, verssorból legenerálhatók). A felhasználói igények, az informatikai szolgáltatók, illetve az informatikai eszközök lehetőségeinek csomópontjában az alábbi tárca típusok alakultak ki:

A csoportosítás a csomópont teljessége alapján:

- a) Teljes csomópont (tartalmazza a teljes blokkláncot);
- b) Könnyű (light)tárca (nem tárolják a blockchain teljes másolatát).

Csoportosítás az online lét alapján:

- a) A forró tárca („hot wallet”) (folyamatosan az internethez kapcsolódik);
 - aa) Web alapú tárcák – egy szolgáltató webes felületén elérhető;
 - ab) Desktop tárcák – a privát kulcsot a számítógépen tárolják;
 - ac) Mobil tárcák – a privát kulcsot a mobiltelefonon tárolják;
- b) Hideg tárolás avagy offline kriptovaluta tárca;
 - ba) Papír alapú tárcák – kinyomtatott kulcspárok;
 - bb) Hardver tárca – speciális pendrive-hoz hasonló eszközök-

További tárca csoportok:

- a) Brain avagy „agy” tárca – a kulcsok, vagy a kulcsok alapjául szolgáló szavakat a felhasználó megjegyzi;
- b) Többszörös identifikációs kriptovaluta tárca²⁹ – több privát kulcs egyidejű használata szükséges a tranzakció lebonyolításához. A „multisig” tárca csak

²⁶ Bővebben: <https://medium.com/@karthikmargabandu7/public-keys-private-keys-and-bitcoin-address-bf26125addf7> vagy <https://bitcoin.hu/archivum/bevezeto/hogyan-mukodik-a-bitcoin/a-bitcoin-cimek-technikai-hattere/>

²⁷ Az elgépelések, félreértések elkerülése érdekében a Base58Check egyéni kódolási képletet használja, amely nem használja a 0, a O, az I és az l karaktereket és tartalmaz magában ellenőrző karaktereket is a pontatlanság elkerülése érdekében.

²⁸ Például: 1FsGty1hk4HoXAVEXGV73GeVdXnec8SjUt

²⁹ FRANCO, Pedro: Understanding Bitcoin: Cryptography, engineering and economics. Wiley, 2015. 84. o.

akkor engedélyezi a kriptovaluták küldését, ha azt elegendő számú privát kulccsal igazolást kap – az előre meghatározott kulcsok közül. Ez utóbbi tárca típus a hatósági felügyelet alatt álló kriptovaluták tárolására is alkalmas, hiszen így jelentősen csökkenthető annak az esélye, hogy a lefoglalt kriptopénzekkel a hatóság bármely tagja önállóan sajátjaként rendelkezzen.

4. A kriptovaluták további ismérvei

A kriptovaluták és a hozzájuk kapcsolódó tárcák ismertetése után tehát két fontos tulajdonságukat kell kiemelni: korlátozott számban érhetőek el és egy adott pillanatban csak egy helyen/egy tárcában létezhetnek.

Ha ezen tulajdonságok bármelyike sérül, akkor kriptovalutába vetett bizalom azonnal megrendül és az a kriptovaluta végét jelentené, de ilyenre eddig az ismert kriptovalutáknál még nem került sor.

Az elmúlt időszakban a kriptovaluták és a létező legális pénzügyi rendszer közé számos innovatív kapcsolatot létesítettek. Van olyan szolgáltatás, ahol ingyenesen lehet bankszámlát nyitni és az arra utalt, vagy bankkártyával feltöltött összegből bitcoin vásárolni. Lehetséges teljesen ingyenesen Visa kártyát igényelni³⁰ és a hozzá kapcsolódó telefonos applikációval folyamatosan lehet a kriptovalutánkat visszaváltani és devizaautalásokat, vagy kártyás fizetéseket teljesíteni.³¹ Vannak olyan szolgáltatások is, amelyek lehetővé teszik, hogy egy Visa bankkártya mögött elhelyezett betéti számlához egy bitcoin tárcát ad a szolgáltató és a bankkártyás fizetés mellett a rendszer átváltja aktuális árfolyamon a bitcoin és teljesíti a kártyás fizetést³².

Mindezen szolgáltatások azonban messze nem olyan népszerűek, mint a hagyományos kártyás fizetési eljárások és a feltörekvő cégek sokszor jelentős díjat számítanak fel a szolgáltatásaikért. Valahol a kriptovaluta eladási és vételi ára közti különbözettel, valahol a kriptovaluta transzferálásának költségével.³³

A tendencia azonban jól látható: a hagyományos – és a felhasználók számára könnyen kezelhető – pénzügyi szolgáltatások közé bekerülnek a kriptovaluták is

³⁰ Jelen tanulmányban számos szolgáltatás kerül említésre, de ezek nem a promótálást szolgálják, hanem csupán a szolgáltatások széles körére kívánnak példákat bemutatni.

³¹ Ilyen például a revolut.com, – viszont a vásárolt bitcoin nem egy általunk ismert tárcában jelenik meg. Az ügyfél csak az egyenleget ismeri és a kriptovalutát nem is transzferálhatja. E szolgáltatásban a bitcoin kincsképző pénz funkciót lát el.

³² Ilyen például a SpectroCoin VISA Debit Card, vagy www.coinizy.com/; coinsbank.com/; www.bitwala.io/; xapo.com/; cryptopay.me; wirexapp.com; www.advcash.com/en/.

³³ Nem ritka az 1%, vagy 0,0025BTC költségként megjelölve (a kettőből a magasabb)

olyan módon akár, hogy a felhasználóknak semmilyen ismerete nincs a blokklánc technológiáról.

A kriptovaluták egyik fő értéke, hogy gyorsan, szinte azonnal teljesebbé mennek a tranzakciók. A valóság azonban nem teljesen ezt igazolja. A bitcoin esetében az az időszak, amikor a tranzakció véglegesen a blokkláncra kerül 2018. évben 5-10 perc, de jelentős forgalom esetén volt, amikor ez 29³⁴ percig tartott. A rendszer leterheltségétől és a felajánlott díjtól függ, hogy mennyi idő alatt kerül fel a blokkláncra a tranzakció. Ez a múltban extrém esetben akár 16 óra is volt.³⁵

Egy kutató cég, – amely a különböző kriptovaluták piacán végzett tevékenységeket vizsgálja, – becslése szerint 2,78 és 3,79 millió közötti, vagyis az összes bitcoin 17-23 százaléka elveszett. Számos módon lehet elveszíteni a bitcoint. Lehetséges, egyszerűen elveszíteni a privát kulcsot vagy az azt tároló eszközt,³⁶ de hibás programok futtatása, vagy szoftverhibák is vezethetnek ilyen eredményre. A bányászat során számos lehetőség van az érmék elvesztésére: például a díjak lehívásának elmulasztása. Az is a kriptovaluták végleges elégetését jelenti, ha valaki olyan tárcára utal, amelyhez nincsen senkinek hozzáférése.³⁷

A nyomozóhatóságok számára is lehetőség a kriptovaluták tranzakciós listájának – főkönyvének – értékelése, elemzése. A blokkláncban szerepelnek az adatok. Vannak publikus oldalak – legfőképpen a bitcoin-ra³⁸ – amelyekből könnyen és felhasználóbarát módon lehet információt gyűjteni. Ilyenek a <https://explorer.bitcoin.com> <https://blockchain.info/hu> <https://blockexplorer.com>,³⁹ ahol a tárcák publikus címeinek ismeretében megnézhetjük a tranzakciók listáját, az összes érkezett bitcoin mennyiségét és az aktuális egyenleget.⁴⁰

Nagyon fontos kiemelni azonban, hogy az anonimitás csupán viszonylagos a kriptovaluták világában; bár az adott címek használói alapvetően teljesen ismeretlenek, azonban a címek közötti utalások iránya, azok ideje és nagysága minden-

³⁴ Bővebben: <https://blockchain.info/hu/charts/median-confirmation-time?timespan=all>

³⁵ BUCHKO, Steven: How long do bitcoin transactions take? <https://coincentral.com/how-long-do-bitcoin-transfers-take/> [2018.06.02.]

³⁶ Ennek egyik leghíresebb esetét James Howells, a londoni informatikus, aki elvesztette a 7500 bitcoint, vagyis körülbelül 56 millió dollárt, amikor laptopját 2013-ban eldobták. Elon Musk is tett olyan nyilatkozatot, hogy elfelejtette, hogyan érheti el digitális érméinek egy részét.

³⁷ MATSAKIS, Louise: How Wired lost \$100,000 in bitcoin, https://www.wired.com/story/wired-lost-bitcoin/?mbid=BottomRelatedStories_Sections_5 [2018.06.02.]

³⁸ A második legértékesebb kriptovaluta az Ethereum elérhető a www.etherscan.io oldalon.

³⁹ Nem csak a bitcoin blokkláncra tekinthető meg: <https://etherscan.io/> <https://chainz.cryptoid.info/>.

⁴⁰ Megtekinthetjük, hogy például a WikiLeaks tárcájára (más forrásból megismert tárca nyilvános kulcsa: 1BTCorgHwCg6u2YSAWKgS17qUad6kHmtQW) 2018. június 1-ig több mint 5884 BTC érkezett, de kevesebb, mint 1 található rajta.

ki számára látható. Ezért is nevezik a rendszert sokszor inkább pszeudonimnak,⁴¹ hiszen ha a tranzakciók láncolatában egyetlen címet is sikerül valamilyen módon valós személyhez kötni, onnantól fogva az egész utalástörténete (ideértve a jövőbeli tranzakcióit is) ismertté válik a nyomozó hatóság előtt.⁴²

A legújabb tendencia szerint azonban a tárcákat az anonimitás fokozása érdekében tovább fejlesztették. Van olyan mobiltárca, amelyik mindössze 10 bitcoin címet cserélget véletlenszerűen (mindenkinek egyénileg a saját tárcájában), míg más tárcák minden egyes tranzakcióhoz egy teljesen új bitcoin címet generálnak.

A nyomozások során a kriptovaluták globális jellege folytán azonban a blokk-láncban szereplő és a hatóságok számára ismert személy ugyanúgy lehet az utca végén, ahogy a föld másik sarkában. A kriptovalutákat a felhasználók egyre inkább a mindennapi ügyletekhez is használják (földrajzi helyhez kötődő áru vásárlása, vagy szolgáltatás igénybevétele),⁴³ ezen túlmenően pedig egyre több kriptovaluta tárcakezelő szolgáltató csak olyan ügyfél tranzakcióit hajtja végre, aki email címes azonosításon kívül okmányaival igazolta magát, vagy legalább telefonos azonosítást is megvalósított, így gátolva a pénzmosás jellegű bűncselekményekben való közreműködést.

A minden egyes utaláshoz egyedi kulcspár létrehozatalát megelőzően is beindítottak olyan szolgáltatásokat a kriptovalutával foglalkozó személyek, amelyeknek az a célja, hogy a kriptovaluta eredetét a blokk-láncban követhetlenné tegye. Ezt olyan módon valósítják meg, hogy egy-egy nagyobb mennyiségű tranzakcióban érintett kriptovalutát egy tárcába transzferálják, majd – némi szolgáltatási díjért cserébe – a nagy közös összegből utalják tovább a kriptovalutákat akár kisebb összegekben is – így érve el az összegek követhetlenségét.

Fontos a nyomozóhatóságok és a titkosszolgálatok hatékony megelőző, felderítő jellegű tevékenysége.⁴⁴ Ahogy egyes anonimizáló proxy szerver, vagy TOR hálózat exit node-ot is (minden bizonnyal) titkosszolgálatok üzemeltetnek, úgy érdemes ezeket a szolgáltatásokat is létrehozni az abból megszerezhető információk érdekében.

⁴¹ Lásd MÖSER, Malte: Anonymity of Bitcoin Transactions. 2013. 1. o. <https://www.wi.uni-muenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf> [2018.04.24]

⁴² HALÁSZ Viktor: Kriptovaluták a bűnüldözésben – új kihívások és lehetséges válaszok (Diplomamunka). NKE NETK 2018. 24. o.

⁴³ Bővebben: <https://coinmap.org>

⁴⁴ KOVÁCS Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, Phd értekezés 114.o.

5. Mekkora a veszélyeztetettség?

A kriptovaluták piaci értéke nagyon nagy volatilitást mutat. A közismert kriptovaluták esetében is sokszor volt 10%-ot meghaladó árfolyamváltozás egy napon belül is.

E cikk írásának időpontjában a bitcoin a legértékesebb kriptovaluta és bár volt már az árfolyama 20.000 USD környékén is – jelenleg 7.364 USD-on áll. Ez piaci kapitalizációban⁴⁵ azt jelenti, hogy valamivel több, mint 34.000 milliárd forintot érnek ezek a kriptovaluták.⁴⁶

Ezek az összegek meglehetősen nagyok, de nagyon nagyszámú személy tulajdonában vannak – a tulajdonosi szerkezet heterogén.

Annyit lehet feltételezni, hogy a bitcoin rejtélyes és a mai napig ismeretlen feltalálója/fejlesztője Satoshi Nakamoto a mai napig tulajdonol hozzávetőleg 1 millió bitcoint⁴⁷. Ezek a kriptovaluták a 2009. január 3-ai indulást követően kialakultak⁴⁸, de az óta változatlanul vannak ugyanazon tárcákban⁴⁹. Ha valamilyen oknál fogva a feltaláló(k) értékesítenék ezeket a bitcoinoikat, azt mindenki észrevehetné, hiszen a blokkláncból ez látható.

A bitcoin – mint a legjelentősebb kriptovaluta – becsült tranzakciós értéke naponta e cikk írása során – amikor az árfolyam a korábbi legmagasabb ár körülbelül harmada – is egy milliárd USD körül mozog. Jelen fejezet írása során a létrehozott bitcoin tárcák száma meghaladta a 25 milliót.⁵⁰

A kriptovaluták a blokklánc technológiának csupán egyik megvalósulási formái. A blokklánc technológia azt teszi lehetővé, hogy egy központi szerver működése nélkül egy egyenrangú hálózatban információk láncolata alakuljon ki olyan módon, hogy a korábban közölt információk integritása vitathatatlan.

E mellet fontos tulajdonság, hogy a blokkláncba információt felfűző entitások egyenrangúak.

⁴⁵ Bővebben: <https://blockchain.info/hu/charts/market-cap> – Market Capitalization

⁴⁶ Viszonyítási alapként Magyarország költségvetésének 2018. évi bevételi főösszege 18.751 milliárd forint, és a forgalomban lévő forint bankjegyek értéke 2016. évi adatok szerint 3.365 milliárd forint. A Shell óriásvállalat 2017. évben (piaci kapitalizáció jelenértéken) 62.000 milliárd forintot ért, az Allianz 22.576 milliárd forintot.

⁴⁷ Egyes vélemények szerint 1.148.800 BTC áll a tulajdonában, amivel bőven a leggazdagabb emberek 10-as listájába is bekerült árfolyamtól függően (bővebben <https://news.bitcoin.com/people-keeping-satoshi-nakamoto-bitcoin/>)

⁴⁸ KLITZKE, Evan: How Many Bitcoins Did Satoshi Nakamoto Mine? <https://eklitzke.org/how-many-bitcoins-did-satoshi-nakamoto-mine> [2018.05.27.]

⁴⁹ WILE, Rob: Bitcoin's Mysterious Creator Appears to be Sitting On a \$5.8 Billion Fortune. <http://time.com/money/5002378/bitcoin-creator-nakamoto-billionaire/> [2018.05.27.]

⁵⁰ <https://blockchain.info/hu/charts/my-wallet-n-users> [2018.06.02.]

A más területeken történő alkalmazhatóság folyamatosan foglalkoztatja fintech cégeket, pénzügyi vállalkozásokat, feltalálókat és állami szereplőket.

Vannak teljesen új megoldások, amelyek egyfajta új helyi pénzt hoznak létre a blokklánc technológia segítségével úgy, hogy az akár minden internettel kapcsolatban álló ügyfél számára elérhető.⁵¹

A blokklánc technológia számos fejlesztési lehetőséget nyitott meg. A nagy pénzügyi szolgáltatók is vizsgálják annak lehetőségét, hogy miként tudják rendszereik hatékonyságát növelni használatával.⁵²

Amikor arra van szükség, hogy bizonyos információ megváltoztathatatlanul rendelkezésre álljon a felhasználók széles tábora számára és azt egy központi egység kompromittálásával ne lehessen befolyásolni, akkor megoldást jelenthet a blokklánc technológia.

Ukrajnában és Grúziában⁵³ a közigazgatási rendszer egyes elemeit – például a földhivatali nyilvántartást – a blokklánc technológiára alapítva fejlesztik.⁵⁴ Észtország forradalmian új tervekkel 2017-ben közzétette, hogy az Euro-hoz kötött nemzeti kriptovalutát kíván kibocsátani⁵⁵, de végül bejelentette, hogy nem valutaként kívánják bevezetni az EstCoin-t, hanem az e-állampolgárságot támogató informatikai rendszerként⁵⁶.

Ha elképzelünk egy olyan rendszert, amelyben minden személy, aki előzetesen azonosította magát (pl.: ügyfélkapun keresztül történő azonosítás) egy blokklánc technológián alapuló közzétételt tudna eszközölni arról, hogy eltulajdonították a gépjárművét. Egy egyenrangú hálózatban ez az információ gyorsan szétterjed minden címzettnek, így akár egy közlekedési csomópontban üzemelő rendszámfelismerő rendszernek, ahol aztán jelzés indulhat a rendészeti szerveknek a szükséges intézkedések megtételére.⁵⁷

⁵¹ Ilyen például a Mycelium Card, amely az összes szükséges hardver elemet is kifejlesztette a fizetési megoldásához – bővebben: <https://card.mycelium.com/>

⁵² <https://entethalliance.org/enterprise-ethereum-alliance-becomes-worlds-largest-open-source-blockchain-initiative/> [2018.06.10.] illetve <https://bitport.hu/ma-mar-nem-az-it-cegek-mondjak-meg-mit-kell-vasarolnia-egy-banknak> [2018.06.10.]

⁵³ Jellemzően az esetleges jogellenes, vagy korrupciós okból bekövetkező módosítások megelőzése érdekében.

⁵⁴ <https://www.reuters.com/article/us-ukraine-bitfury-blockchain/ukraine-launches-big-blockchain-deal-with-tech-firm-bitfury-idUSKBN17F0N2?il=0> [2018.06.10.]

⁵⁵ <https://www.ccn.com/estcoin-estonia-could-soon-launch-its-own-digital-currency/> [2018.06.10.]

⁵⁶ <https://www.bloomberg.com/news/articles/2018-06-01/estonia-curbs-cryptocurrency-plan-that-drew-rebuke-from-draghi?srnd=cryptocurrencies> [2018.06.10.]

⁵⁷ Az ötlet logikusnak tűnik, de a megvalósítást illetően megoldható volna a hagyományos szerverkliens kapcsolaton keresztül is, így előnye annyi maradna, hogy bármelyik csomópont kiesése esetén

Egy másik problémával kapcsolatban is működőképes megoldást jelenthetne a blokklánc technológia: a gépjárművek kilométer órájának visszatekerése szer- te Európában komoly gondot okoz. Ha azonban kialakításra kerül egy rendszer, amelyben minden regisztráló gépjárműhöz egy kulcspárt kerül hozzárendelésre és számos autószerelő műhely, műszaki vizsgaállomás, vagy akár benzinkút megkap- ja a jogot, hogy a nyilvános kulcshoz tartozó blokkra információt fűzzön, akkor a tulajdonosnak a gépkorcsi értékesítésekor hiteles és megváltoztathatatlan blokklánc információ állna a rendelkezésére a privát kulcs felhasználásával, hogy milyen a jár- mű futásteljesítménye, milyen szerviz beavatkozásokat hajtottak rajta végre, de akár hogy mennyi volt jellemzően a fogyasztása.

Nem meghatározható, hogy a kriptovalutákkal összefüggő növekvő tendenciá- nak mekkora hányada kapcsolódik Magyarországhoz, de a különféle szolgáltatások, internetes fórumok, médiamegjelenések azt mutatják, hogy hazánkban is egyre je- lentősebb a kriptovaluták irányába megjelenő figyelem.

Fontos azonban azt is megjegyezni, hogy a Satoshi által lefektetett elvek sze- rint működő bitcoin sem egy végleges és változtathatatlan produktum. Ahogy az internet megalkotói sem gondoltak arra, hogy mekkora fejlődésen fog átesni a világháló,⁵⁸ úgy az eredeti tervek is megváltoztak. Ezt a változást egy nem teljesen egységes fejlesztői csoport valósítja meg.⁵⁹ Bár a forráskód nyilvános, de a további fejlesztések eredményezhetik a bitcoin rendszerének hibáit és akár hanyatlását is.

Összességében tehát látható, hogy:

- a kriptovaluták jelentős változást hoztak a pénzügyi kultúrában,
- a blokklánc technológia az élet számos területén ad forradalmian új megoldá- sokat.

Van, aki befektetési jelleggel, van, aki a technológiai újdonságok felé tanúsított érdeklődéssel, és van, aki a bűnös vagyonának elrejtésére, vagy más bűnös tevékeny- ség céljaként, vagy eszközöként tekint a kriptovalutákra. Témánk szempontjából a bűncselekményekhez való kötődése érdemel kiemelés.

is tökéletesen működőképes maradna és az ügyfelek azonnal meg tudnák osztani az információkat.

⁵⁸ Az internet hajnalán még elképzelhetetlennek tartották, hogy az IPV4-es IP címek valaha elfogy- hatnak, vagy hogy az internet ennyire átfórmálja a gazdaság és a modern társadalmak működését.

⁵⁹ The Bitcoin Foundation, Inc. nevű szervezet legfőbb célja Satoshi Nakamoto elveinek tovább foly- tatása, fejlesztése, népszerűsítése. <https://bitcoinfoundation.org/website-terms-service/> [2018.06.08.]

6. Rendészeti kihívások, válaszok

A kriptovaluták piaci kapitalizációja tehát jelenleg nem jelentős. Ha a blokklánc technológiába vetett bizalom megrendül, akkor a XIX. századi aranyláz könnyen lecsenghet.

A bitcoin árfolyamának alakulásában az árfolyamcsökkenések mögött jellemzően a bizalomvesztés jelent meg:

- egyes bitcoin brókereket ért támadások, általuk elkövetett visszaélések,⁶⁰
- állami szabályozók negatív hatása – jellemzően elfogadás tiltása – szintén hátrányos a kriptovaluta megítélésére,⁶¹
- más kriptovaluták irányába elmozduló érdeklődés,
- a kriptovalutát működtető informatikai háttérben való bizalomvesztés⁶²

Nem kell konspirációs teóriákra gondolnunk, ha azt feltételezzük, hogy a pénzügyi szolgáltatók intézkedéseket tesznek, vagy akár lobbiznak annak érdekében, hogy a kriptovaluták elfogadhatósága csökkenjen. A pénzügyi eszközök bankrendszerrel független tárolása, kezelése, transzferálása számukra bevétel kiesést eredményezhet. Jelentős érdekek léteznek az irányba, hogy a blokklánc technológia és a kriptovaluták a bankrendszeren belülre kerüljenek, vagy elfogadhatóságuk csökkenjen.

Állami oldalról egyrészt támogatandó minden innovatív technológia, amely a polgárok jóléte irányába hat⁶³, de csak addig a mértékig, amíg a hátrányok ezt meg nem haladják. Melyek lehetnek ezek:

- a bankrendszer bevételeinek csökkenése által az állami bevételek csökkenése,⁶⁴
- a technológia használatában fejlettebb szinten álló külföldi szolgáltatóknál jelentkeznek inkább bevételként a kriptovalutákhoz kapcsolódó költségek,⁶⁵
- ha a technológia nem váltja be a hozzá fűzött reményeket, akkor az erre a célra elköltött javak nem térülnek meg, így összgazdasági hátrányt okoznak,

⁶⁰ Bővebben lásd: <https://cointelegraph.com/tags/mt.gox>

⁶¹ Bővebben például: <https://economictimes.indiatimes.com/wealth/personal-finance-news/your-bank-will-not-allow-you-to-buy-bitcoins-anymore/articleshow/63627123.cms>

⁶² Példaként említhető az ún. DAO csalás – bővebben: <https://www.coindesk.com/understanding-dao-hack-journalists/>

⁶³ Bizonyos feladatok költséghatékony, visszaélésektől mentes ellátása pl. a korábban említett célokra.

⁶⁴ Természetesen itt kérdésként merül fel, hogy az ügyféli oldalon jelentkező költségsökkenésből származó megtakarításait mire fordítják az ügyfelek

⁶⁵ Itt a kedvező külkereskedelmi és fizetési mérlegre merkantilista szempontból tekintve mindenképpen előnyös a fejlettebb államok számára

- az állampolgárok kriptovalutákkal összefüggésben elveszítik anyagi javaik egy részét⁶⁶.

Ezen problémák elhárításában, megszüntetésében a rendészeti szerveknek érdemben nincs tennivalójuk, de melyek azok a hátrányos folyamatok, melyek feladatot adnak?:

- Az elmúlt években az Europol az internetes szervezett bűnözői fenyegetettségről szóló jelentéseiben is felhívta a rendvédelmi szervek fokozott figyelmét arra, hogy a kriptovaluták bűnelkövetési célú felhasználása egyre gyakoribb.⁶⁷
- A kriptovalutákhoz köthető bűncselekmények sértettjévé válhatnak az állam polgárai, illetve vállalkozások (csalások⁶⁸, információs rendszerek elleni támadások⁶⁹, tőkepiac-felügyeleti intézkedések hiánya). Ebben a körben bűnmegelőzési kampányok indítása volna célszerű a kriptovalutákhoz kapcsolódó piaci szereplők bevonásával olyan felületeken, amelyeket a lehetséges sértettek látogatnak – például kriptovalutákkal foglalkozó weboldalakon, fórumokon, szakmai rendezvényeken.
- A kriptovaluták anonimizáló, és földrajzi határokra érzéketlen tulajdonságainak kihasználása a bűnelkövetés során (pl. zsaroló vírusok⁷⁰, pénzmosás⁷¹, terrorizmus finanszírozása).
- A bűnös forrásból származó vagyon elrejtése kriptovalutákban.

Ezen utóbbi problémák elleni fellépésben a bűnüldöző szervek további hatékony lépéseket kell tegyenek:

- Szükséges részt venni a jogalkotásban annak érdekében, hogy a kriptovalutákkal kapcsolatos szolgáltatások nyújtását magyar vállalkozások is jogszerűen és megfelelő ellenőrzés mellett végezhessék.⁷²

⁶⁶ Itt nem jogsértő cselekményekre, hanem helytelen döntésekre, a piac várható mozgásának helytelen prognosztizálására kell gondolnunk

⁶⁷ Lásd EUROPOL: Internet Organised Cybercrime Threat Assessment 2014-2018.

⁶⁸ Lásd ESZTERI Dániel: Egy bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és jog 2017/1. 25-31. o.

⁶⁹ ESZTERI Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén és a tulajdon helyzetének magán- és büntetőjogi elemzése virtuális közösségekben. Doktori értekezés. Pécs, 2015. 204-207. o.

⁷⁰ NAGY Zoltán András – MEZEI Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa In: Gaál Gyula – Hautzinger Zoltán (szerk.) Szent Lászlótól a modernkori magyar rendészettudományig. Pécsi Határőr Tudományos közlemények 19. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2017. 165. o.

⁷¹ NAGY Zoltán András – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog 2018/1. 27-28. o.

⁷² Ne legyen szükség más államokban (pl. Anglia) létesített vállalkozások fióktelepeként működtetni a vállalkozásokat.

- A létrejövő és a pénzügyi rendszerbe becsatlakozó fintech cégekkel partneri viszony kialakítása és közös elemző-értékelő rendszerek működtetése a pénzmosság gyanús tranzakciók kiszűréséhez.
- Az új büntetőeljárásról szóló 2017. évi XC. törvény nevesíti az elektronikus adatot mint bizonyítási eszközt, valamint a rendelkezései alapján lehetővé válik az olyan virtuális vagyonelemek lefoglalása, mint a bitcoin vagy az elektronikus pénz speciális formái. Az új szabályozásnak köszönhetően a fizetésre használt elektronikus adat lefoglalását úgy is végre lehet hajtani, hogy az elektronikus adattal olyan műveletet végeznek, amely az érintettnek az elektronikus adattal kifejezett vagyoni érték feletti rendelkezési lehetőségét megakadályozza.⁷³ Azonban a büntetőeljárásokban⁷⁴ felmerülő kriptovaluták lefoglalása, kezelése érdekében szükséges egy módszertani utasítás kimunkálása az ügyészséggel közösen, az egységes joggyakorlat megteremtése érdekében.
- Szükséges a blokklánc technológiához kapcsolódó ismeretek elmélyítése a bünyildöző és titkosszolgálati szervek állományában.⁷⁵
- Fontos kiaknázni a bünyildözési célú nemzetközi együttműködésből származó lehetőségeket: megismerni a legjobb gyakorlatokat, esettanulmányokat, részletszabályozási megoldásokat, használni a közös erőforrásokat.⁷⁶

Stratégiai szinten az egyes államok számára fontos az összehangolt magatartás. Megítélésem szerint nem jelent megoldást a kriptovaluták túlzott tiltása, mivel azok a bünyelkövetéshez történő felhasználást csupán megnehezítik, de emellett nehezen felderíthetővé is teszik. Szükséges a törvényi szigorítás, de nem olyan mértékben, hogy az az innováció elfojtása mellett az elkövetők konspirációjához vezessen, ha-

⁷³ Be. 315. § (1) és (2) bekezdései; Lásd bővebben az elektronikus adat lefoglalásáról és megőrzéséről: CZINE Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Bünyetöljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.

⁷⁴ Lásd SZATHMÁRY Zoltán: Az elektronikus pénz és a bitcoin biztosítása a bünyetöljárásban. Magyar Jog 2015/1. 639-647. o.; valamint DORNFELD László: A kibertérben elkövetett bünycselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2. 125-126. o.

⁷⁵ Lásd ehhez FURNEAUX, Nick: Investigating cryptocurrencies – Understanding, extracting and analyzing blockchain evidence. Wiley, 2018.

⁷⁶ Lásd bővebben az európai és nemzetközi erőfeszítésekről a kibertér védelme érdekében: PARTI Katalin – KISS Tibor: Az informatikai bünyözés. In: Borbíró Andrea – Gönczöl Katalin – Kerecsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft., 2017. 510-514. o.; SZONGOTH Richárd – VETTER Dániel: Nemzetközi bünyügyi együttműködés a kiberbünyözés területén. Belügyi Szemle 2018/7-8. 7-21. o.; Továbbá például az Európai Rendőrség (Europol) EC3 blokklánc elemző platformját vagy a United Nations Office on Drugs and Crime (UNODC) képzéseit: <https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>

nem olyan mértékben, hogy abból a bűnüldöző és titkosszolgálati szervek információt szerezhessenek.

Mekkora erőforrást kell delegálni a rendészeti szervek részéről a kriptovaluták-kal kapcsolatos problémák orvoslására? Sajnos azt nehéz meghatározni. Azonban az tény, hogy 2012. és 2017. között 141 ügy kapcsolódott a kriptovalutákhoz, ami összességében nem magas szám, de az emelkedés a 2012. évi 1 büntetőügyhöz képest a 2017. évi 58 ügy egy exponenciálisan emelkedő görbét mutat.⁷⁷

Vélhetően a következő években sem valósulnak meg a kriptovalutákkal kapcsolatban olyan bűncselekmények, melyek Magyarország gazdasági érdekét érdemben befolyásolnák, hiszen nem nagy az ország kitettsége. Azonban az valószínűsíthető, hogy nagyszámú sértettet érintő jogsértések kerülhetnek napvilágra. Ezen túlmenően az is fontos szempont kell legyen, hogy az állampolgárok nyomozóhatóságokba vetett bizalmát és megbecsültségét nagyon pozitívan befolyásolná, ha az ilyen ügyeket szakértő módon, gyorsan és eredményesen fejeznék be a hatóságok.

FELHASZNÁLT IRODALOM

- BAKÓ Tamás: Bitcoin hálózatok elemzése (Diplomamunka). Eötvös Loránd Tudományegyetem, Természettudományi Kar, Matematikai Intézet 2015.
- CZINE Ágnes: L. fejezet – A lefoglalás. In: Belegi József (szerk.): Büntetőeljárás jog I-II. – új Be. – Kommentár a gyakorlat számára. HVG-ORAC Lap- és Könyvkiadó Kft. Budapest, 2018.
- DORNFELD László: A kibertérben elkövetett bűncselekményekkel összefüggésben alkalmazható kényszerintézkedések. Belügyi Szemle 2018/2.
- ESZTERI Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécs, 2015.
- ESZTERI Dániel: Egy bitcoinnal elkövetett vagyon elleni bűncselekmény és az ahhoz kapcsolódó egyes jogi kérdések. Infokommunikáció és jog 2017/1.
- EUROPOL: Internet Organised Cybercrime Threat Assessment 2014–2018.
- FRANCO, Pedro: Understanding Bitcoin: Cryptography, engineering and economics. Wiley, 2015.
- FURNEAUX, Nick: Investigating cryptocurrencies – Understanding, extracting and

⁷⁷ Készenléti Rendőrség – Nemzeti Nyomozóiroda – Kiberbűnözés Elleni Főosztály témakutatásából.

analyzing blockchain evidence. Wiley, 2018.

HALÁSZ Viktor: Kriptoaluták a bűnüldözésben – új kihívások és lehetséges válaszok (Diplomamunka). NKE NETK 2018.

KOVÁCS Zoltán: Az infokommunikációs rendszerek nemzetbiztonsági kihívásai, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, PhD értekezés
MÖSER, Malte: Anonymity of Bitcoin Transactions. 2013.

NAGY Zoltán András – MEZEI Kitti: A zsarolóvírus és a botnet vírus mint napjaink két legveszélyesebb számítógépes vírusa In: Gaál Gyula – Hautzinger Zoltán (szerk.) Szent Lászlótól a modernkori magyar rendészettudományig. Pécsi Határőr Tudományos közlemények 19. Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, 2017.

NAGY Zoltán András – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog 2018/1.

PARTI Katalin – KISS Tibor: Az informatikai bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerecsi Klára – Lévay Miklós (szerk.): Kriminológia. Wolters Kluwer Kft., 2017.

SZATHMÁRY Zoltán: Az elektronikus pénz és a bitcoin biztosítása a büntetőeljárásban. Magyar Jog 2015/1.

SZONGOTH Richárd – VETTER Dániel: Nemzetközi bűnügyi együttműködés a kiberbűnözés területén. Belügyi Szemle 2018/7-8.