DOI: 10.38146/BSZ.2018.7-8.9

HALÁSZ VIKTOR

A bitcoin működése és lefoglalása a büntetőeljárásban

„Az elektronikus pénznek egy teljességgel egyenrangú felek között működő változata lehetővé tenné a küldő és a fogadó fél közötti közvetlen online fizetést bármiféle pénzintézet közbeiktatása nélkül."[1]

Az idézett felvetéssel indul a bitcoin működését leíró tanulmány, amely a 2008-as gazdasági világválság közepén jelent meg a világhálón.[2] A tanulmány egy olyan több évtizedes problémára adott megoldást, ami már a nyolcvanas évek óta foglalkoztatta a világ kriptográfusait: hogyan lehetséges olyan fizetési rendszert alkotni, amelyben a felek közvetlenül továbbíthatnak értéket egymásnak anélkül, hogy ehhez meg kellene bízniuk egy harmadik, közvetítő félben?[3]

A mindennapi élet online térbe áthelyeződésével szükségszerűen felvetődött a digitális értéktovábbítás mikéntjének kérdése is. Az információ digitális továbbítása során valójában ugyebár sosem az eredeti adat kerül egyik helyről a másikra, hanem csupán másolat készül az adatról az új helyen is. Az esetek túlnyomó részében ez nem okoz gondot, hiszen – például – egy kép küldése során az egyetlen cél, hogy az a fogadó félnél megjelenjen, és emellett nem bír jelentőséggel, hogy a kép egy eredeti példánya a küldő félnél továbbra is rendelkezésre áll.

Értékkel bíró dolog átruházása során azonban az értékhordozó – dolog vagy adat – többszöröződése fel sem vetődhet, hiszen akkor kétszer lehetne elkölteni. Fizikai dolgok átruházása esetén a probléma soha nem is volt jelen, hiszen egy pénzérme (bankó, kötvény, aranytömb stb.) egyszerre csak egy helyen létezhet. A javak fizikai értékhordozók nélküli, „virtuális" továbbítása esetén pedig – már az első, bankszerű intézmények ókori megjelenése óta – szükség volt egy közvetítő félre, akiben mindannyian megbíztak, és aki nyilvántartotta és hitelesen tanúsította a felek rendelkezésére álló vagyon mindenkori mértékét.

1 Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, p. 1. https://bitcoin.org/bitcoin.pdf

2 A tanulmány készítőjének valódi személyazonosságára sosem derült fény; a külvilággal csupán e-mailek és online fórumok útján kommunikált, jó pár éve pedig egyáltalán nem adott életjelet magáról. Valós kilétével kapcsolatban számos nyomozás indult az évek során, lásd például Who is Satoshi Nakamoto? https://blockonomi.com/who-is-satoshi-nakamoto/

3 Andreas M. Antonopoulos: Mastering Bitcoin: Unlocking Digital Cryptocurrencies. 2015, pp. 2–3.

A XX. század vége felé a pénzintézetek – értve ezen nem csupán a bankokat, hanem minden olyan intézményt, amely bármilyen közvetítő szerepet tölt be pénzmozgások terén – tevékenysége is átvándorolt ugyan a digitális térbe, azonban a működésük alapjául szolgáló rendszer gyakorlatilag változatlan maradt.[4] Annyi történt csupán, hogy az addigi papíralapú, vaskos főkönyvek adatai átkerültek egy elektronikus szerverre, ahonnan gyorsabban lehetett ugyan elérni őket, ám a közvetítő felek iránti igény ugyanúgy nem változott.

A bitcoin éppen arra szolgáltatott megoldást, hogy az értéktovábbítás során a láncolatból kiiktassa a közvetítő pénzintézetet, ekképpen pedig olyan rendszert hozzon létre, amelyben a felek csupán egymással állnak kapcsolatban.

A pénzintézet legfőbb funkciója az elektronikus utalások lebonyolítása során, hogy hitelesen igazolja a tranzakciók érvényességét. Mivel minden tranzakciót a pénzintézet kezel, így nem fordulhat elő, hogy ugyanazt az összeget kétszer utalják el egy számláról. A pénzintézet ekképp garanciát szolgáltat a feleknek arra vonatkozóan, hogy a nekik küldött összegeket valóban meg fogják kapni.

A bitcoin esetében nincs semmilyen központi szerv, amely a tranzakciókat ellenőrizné. A pénzintézet ezen alapvető funkcióját itt az úgynevezett blokklánc biztosítja, egy világméretű, nyilvános főkönyv, amely tartalmazza az összes, valaha végrehajtott bitcointranzakciót. Legfontosabb tulajdonságai: decentralizált, anonim, maradandó és utólag megváltoztathatatlan.[5]

Kérdés, hogy ki vezeti ezt a főkönyvet. A bitcoin forradalmiságát éppen az jelenti, hogy a főkönyv vezetése nem egy a hálózat fölött őrködő intézmény felelőssége, hanem a bitcoinhasználók összessége közösen tartja nyilván, hogy kinek hány bitcoinja van éppen – ezért nevezzük ezt a rendszert decentralizáltnak.

Ha valaki szeretne bitcoincímhez jutni, csupán le kell töltenie egy bitcoinklienst[6], amellyel ez után bármilyen mennyiségben generálhat magának címeket. A címek – ha a bankok analógiáját használjuk – a bankszámlaszámoknak felelnek meg, ugyanis ezek tartják nyilván a bitcoin mennyiségét, és ezek ismerete szükséges az egymás közötti utalások lebonyolításához. Minden címhez tartozik egy úgynevezett privát kulcs is, ami egyfajta jelszóként

4 Robleh Ali – Roger Clews – James Southgate: Innovations in payment technologies and the emergence of digital currencies. Bank of England Quarterly Bulletin, vol. 54, iss. 3, 2014, p. 262.

5 Zheng Zibin – Xie Shaoan – Dai Hong-Ning – Wang Huaimin – Xiangping Chen: Blockchain Challenges and Opportunities: A Survey. International Journal of Web and Grid Services, December, 2017, p. 9.

6 Ennek ma már számos változata létezik, azonban a legelső – és azóta is folyamatosan fejlesztett – kliens a https://bitcoin.org/en/bitcoin-core/ webcímen érhető el.

fogható fel: a privát kulcs ismerete szükséges ahhoz, hogy az adott címen lévő bitcoin felett rendelkezhessünk. A bankszámlaszámokkal ellentétben a címek létrehozásához azonban semmilyen adat megadása nem szükséges (hiszen nem is lenne, aki kezelje ezeket az adatokat), így a blokkláncon rögzített tranzakciók mindegyike anonim.

A kliens letöltésével együtt letöltődik a blokklánc is az addig történt összes utalással együtt. Ha valaki új utalást akar kezdeményezni, a tranzakció adatai (milyen címről, milyen címre, mikor és mekkora mennyiségű bitcoin utalása történt) bekerülnek egy nagyobb blokkba, majd az így összegyűlt tranzakciókat átlagosan tízpercenként – egy kriptográfiai folyamat nyomán – hitelesítik, és hozzákapcsolódnak az előző blokkhoz. Ilyen módon a blokkok láncolata jön létre (innen ered a technológia elnevezése is), ami megtalálható az összes felhasználó számítógépén. Az ilyen számítógépek a csomópontok (*node*-ok).

Mivel a blokklánc értelemszerűen folyamatosan változik – új tranzakciókkal bővül –, ezért természetesen csak azok láthatják a teljes blokkláncot, akiknek a számítógépe állandó online kapcsolatban van. Ha a kapcsolat megszakad, akkor a következő indításnál az azóta keletkezett blokkokat utólag le kell tölteni. Éppen ezért azokat, akik egy adott időpillanatban az aktuálisan teljes blokkláncra rálátnak, teljes csomópontoknak (*full node*-oknak) nevezik.[7] A mindenkori teljes csomópontok hálózata felel tehát a blokklánc folyamatos nyilvántartásáért. A blokkláncban foglalt adatok elvesztése csak olyan módon fordulhatna elő, ha a világ legkülönbözőbb részein lévő teljes csomópontok mindegyike egyszerre semmisülne meg. Máskülönben, ha csupán egy csomópont is megmarad, az újonnan csatlakozó kliensek letölthetik belőle a teljes blokkláncot, újabb és újabb teljes csomópontokat hozva létre – ez garantálja tehát a blokklánc maradandóságát.

A tranzakciók említett, blokkonkénti hitelesítését nem a csomópontok végzik – ők csupán gyűjtik a tranzakciókat, majd a hitelesítés után hozzákapcsolják az elkészült blokkokat a lánc végéhez. A hitelesítés egy számításigényes művelet, amit az úgynevezett bányászok végeznek (a bányászathoz szintén nincs szükség másra, mint egy erre szolgáló program letöltésére, amely ez után automatikusan kapcsolódik a blokklánchoz, és felhasználja az adott számítógép erőforrásait). Ennek során a bányászok összegyűjtik az adott blokkban tíz perc alatt felhalmozódott – hitelesítésre váró – tranzakciókat, majd egymással ver-

7 Ezek nagyságrendje folyamatosan nyomon követhető (lásd például https://bitnodes.earn.com/). Jelenleg minden időpillanatban átlagosan tízezres nagyságrendű teljes csomópont található szerte a világon.

senyezve megoldanak egy kriptográfiai feladványt[8], amelynek bemeneti értékeit e tranzakciók adatai, illetve egy további, még az előző blokkban rögzített adatsor szolgáltatja. Az a bányász, aki elsőként számolja ki a feladvány megoldását, megszerzi a jogot, hogy az így kapott értékkel hitelesítse az adott blokkot, majd azt ellenőrzésre felajánlja a csomópontoknak. Bár a feladvány megoldása nagy számítási teljesítményt igényel, annak ellenőrzése egy pillanat alatt elvégezhető, így ha a csomópontok megfelelőnek találják a megoldást, hozzákapcsolják a blokkot a lánc végéhez, és az egész folyamat elölről indul.[9]

A kriptográfiai folyamat funkciója az, hogy szavatolja a blokkok tartalmának utólagos megváltoztathatatlanságát (másképpen fogalmazva: hogy egy korábban már elutalt bitcoint senki se „költhessen el" újra). Ahhoz ugyanis, hogy ez megtörténjen, a „csalónak" meg kell változtatnia az adott tranzakció adatait, ami szükségszerűen hatással lesz az adott blokkra vonatkozó egész feladványra, amit így újra kell számolni. Ez azonban önmagában még mindig nem elég; mivel a feladvány része az előző blokk végeredménye is, így a megváltoztatott blokk után újra kell számolni az összes többi, ez után keletkezett blokkot is. Mivel átlagosan tízpercenként keletkezik egy újabb blokk, ezért a csalónak egy egynapos tranzakció megváltoztatásához is több száz blokkot kellene egyedül megoldania. Természetesen ez nem lehetetlen (bár valószerűtlenül sok számítási kapacitást igényel), azonban a csomópontok mindig a leghosszabb láncot fogadják el érvényesnek.

Mivel a csaló szükségképpen hátrányból indul (egy múltbeli blokkot akar megváltoztatni), mindeközben pedig tízpercenként újabb blokkok is keletkeznek, ezért csak akkor lenne esélye utolérni és megelőzni az eredeti láncot, ha az összes bányász által biztosított számítási kapacitás legalább több mint a felével rendelkezne.[10]

8 A kriptográfiai probléma egy úgynevezett hash függvény kiszámolását jelenti. A hash függvények lényege, hogy segítségükkel bármilyen mennyiségű adatból (ami esetünkben a hitelesítendő tranzakciók és az előző blokk adatai) képezhető egy meghatározott hosszúságú, ámde rövid hash érték, ami egyfajta ujjlenyomatként is értelmezhető (ugyanazon adathalmaznak mindig ugyanaz lesz a hash értéke). A blokk hitelesítése a kiszámolt hash értékkel történik.

9 Konstantinos Christidis – Michael Devetsikiotis: Blockchains and Smart Contracts for the Internet of Things. IEEE Acces, vol. 4, 2016, pp. 2293–2294.

10 Ez pedig gyakorlatilag lehetetlen, ugyanis jelenleg nem létezik a földön olyan egységes entitás (vállalat, kormány stb.), amely ilyen méretű erőforrásokat birtokolna. A bitcoint bányászó számítógépek összes energiafogyasztása jelenleg megegyezik egy közepes méretű európai ország energiafogyasztásával (Bitcoin's Energy Consumption Can Power An Entire Country. https://www.forbes.com/sites/shermanlee/2018/04/19/bitcoins-energy-consumption-can-power-an-entire-country-but-eos-is-trying-to-fix-that/#1a5b90301bc8), így egy teljes ország az összes energiáját csak és kizárólag bitcoin-bányászatra kellene, hogy fordítsa a sikerhez.

Fontos megérteni tehát, hogy a számításigényesség nem a rendszer szükségszerű velejárója; a tranzakciók akár bányászok nélkül is blokkokba foglalhatók lennének, ha feltételeznénk, hogy a rendszer minden tagja becsületes, és soha senki nem próbálna meg utólag megváltoztatni egy már végbement utalást. Mivel azonban ilyen feltételezésre természetesen nincs mód, ezért a rendszert úgy alkották meg, hogy a blokkok elkészítését szándékosan kriptográfiai műveletek megoldásától tegye függővé, és így a csalás rendkívül energiaköltséges művelet legyen – ily módon valósul meg a blokklánc megváltoztathatatlansága.[11]

Látható, hogy a bitcoin működéséhez két összetevőre van szükség; a blokkláncot nyilvántartó teljes csomópontokra, illetve a hitelesítést nyújtó bányászokra. Jogosan vetődik fel a kérdés, mi késztet bárkit is arra, hogy a rendszer működését valamely szerepben önként fenntartsa (hiszen a bitcoint semmilyen központi szerv nem működteti, az csak a felhasználók önkéntes hozzájárulásával létezhet).

Nos, a teljes csomópont üzemeltetése nem igényel különösebb számítási kapacitást, csupán a blokklánc tárolásához szükséges tárhely és minimális sávszélesség. Ilyen módon önmagában az a tény, hogy valakinek bitcoinja van, érdekeltté teszi őt egy teljes csomópont és ezáltal a rendszer fenntartásában. Ez az elmélet a bitcoin születése után a gyakorlatban is igazolódott (hiszen a rendszer fennmaradt), azóta pedig széles körű infrastruktúra is kiépült a bitcoin köré, így egyre több és több gazdasági szereplőnek is érdekévé válik a fennmaradása.

A bányászat ugyanakkor rendkívül energiaigényes folyamat, így a számítási kapacitás önkéntes biztosítása már a bitcoin indulásakor sem lett volna reálisan elvárható. Éppen ezért a rendszert úgy alkották meg, hogy egy-egy blokk helyes megfejtését elsőként megtaláló bányászt bitcoinnal jutalmazza. Ez egyben választ ad arra a kérdésre is, hogy ki bocsátja ki a gazdasági körforgásban lévő bitcoin „érméket”; az új bitcoinokat a rendszer hozza létre, majd jutalomként kiosztja a sikeres bányászoknak, akik ez után szabadon rendelkezhetnek velük. A jutalom mértéke fix, azonban 210 ezer blokkonként (hozzávetőleg négyévente) feleződik; a rendszer indulásakor egy blokk megfejtéséért még ötven bitcoin járt, ma már csak ennek negyede (12,5 bitcoin), a következő felezés pedig 2020-ban várható.[12]

11 Todor Todorov: Bitcoin: An innovative payment method with a new type of independent currency. Trakia Journal of Sciences, vol. 15, suppl. 1, 2017, p. 164.

12 Nicolas Houry: The Bitcoin mining game. 2014, p. 2. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407834

Ez a metódus megakadályozza, hogy a valuta értéke túlzottan inflálódjon, hiszen idővel egyre kevesebb és kevesebb új bitcoin kerül be a gazdasági körforgásba.[13] Mindemellett az utalások során az utaló feleknek egy bizonyos mértékű tranzakciós díjat is fel kell ajánlaniuk, amire szintén a blokkot hitelesítő bányász válik jogosulttá.[14]

Összefoglalva, tehát a blokklánc egy nyilvánosan elérhető, a hálózat egyenrangú tagjai által közösen vezetett (decentralizált)[15], anonim bejegyzéseket tartalmazó, maradandó és utólag megváltoztathatatlan főkönyv, amely lehetővé teszi annak nyomon követését, hogy kinek milyen mennyiségű bitcoinja van. Ha az internetre úgy tekintünk, mint az információ világméretű hálójára *(world wide web)*, akkor a blokklánc nem más, mint az értékek világméretű főkönyve.[16]

Mi is valójában egy bitcoin?

A bitcoint gyakran ábrázolják fényes érmeként, ami érthető, hiszen az emberi elmének sosem árt egy kapaszkodó, ha valamilyen absztrakt fogalmat kell elképzelnie. És bár mindenki számára nyilvánvaló, akinek legalább csak érintőlegesen is vázolták a bitcoin működését, hogy a rendszerben valódi érmék nem találhatók, a bitcoin mibenlétéről így is sok tévhit kering.

Mint korábban említettem, a bitcoinhálózatban való részvételhez szükség van egy bitcoincímre, illetve a hozzá tartozó privát kulcsra. A cím a bitcoin „tárolására" szolgál, a privát kulcs pedig a címen lévő bitcoinnal való rendelkezéshez szükséges (egyfajta jelszóként). Az előző mondatban idézőjelbe tettem a tárolás szót, ám ha egyszerűen szeretném megfogalmazni a bitcoincímek funkcióját, akkor más kifejezéssel sem jutottam volna sokkal közelebb

13 Ha pedig a csökkenés ütemét függvényként ábrázoljuk, látható, hogy az összes bitcoin mennyisége sosem haladhatja meg a 21 milliót.

14 Nicolas Houry: The economics of Bitcoin transaction fees. 2014, p. 2. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400519

15 Megjegyzendő, hogy a decentralizáltság kapcsán az utóbbi időben egyesekben aggályok merültek fel, ugyanis a rendszer egyre nagyobb energiaigényével párhuzamosan a bányászat az otthoni felhasználóktól egyre inkább áttevődik nagyobb bányászvállalatok kezébe, amelyek így egyre nagyobb önálló szeletet hasítanak ki a bitcoin működtetéséből. Bár a rendszer ettől függetlenül még decentralizált, azonban a folyamat mindenféleképpen egyfajta centralizációnak is tekinthető. Lásd Arthur Gervais – Ghassan O. Karame – Srdjan Capkun – Vedran Capkun: Is Bitcoin a Decentralized Currency? IEEE Security & Privacy, vol. 12, no. 3, 2014, p. 56.

16 Don Tapscott – Alex Tapscott: Blockchain Revolution – How the technology behind Bitcoin is changing money, business, and the world. Penguin Canada, 2016, p. 7.

a valósághoz. A címen ugyanis valójában nem található semmilyen elektronikus érme, vagy más adatcsomag, amit bitcoinnak nevezhetnénk. Egy-egy cím csupán a bitcoinhálózaton a legelső naptól kezdve végrehajtott tranzakciók bizonyos láncolatának éppen aktuális végső eredményét rögzíti, a privát kulcs pedig lehetőséget ad az ismerőjének ezen eredmény – egy újabb tranzakcióval történő – megváltoztatására.

Téves tehát az a széles körben elterjedt nézet, amely szerint a bitcoin valamiféle számítógépes fájl vagy más elektronikus adat.[17] A bitcoin – a megtestesített érték oldaláról vizsgálva – csupán egy absztrakt fogalom, amivel bizonyos tranzakciók láncolatának végeredményét jelöljük[18], és amire nyilvánvalóan szükség van ahhoz, hogy a mindennapok során beszélni tudjunk a rendszer működéséről.

Ha pedig a birtoklás oldaláról szeretnénk megfogni a bitcoin lényegét (mit jelent az, hogy valakinek bitcoinja van?), akkor pedig a privát kulcsot kell a definíció középpontjába helyeznünk: bitcoinja annak van, aki ismer egy (nem „üres") címhez tartozó privát kulcsot, hiszen a bitcoinnal való rendelkezéshez semmi egyébre nincs szüksége. A bitcoin birtoklása tehát nem jelent mást, mint a privát kulcs tudatában lehetőséget[19] arra, hogy valahol az „éterben" létező, és emberek tízmilliói által[20] hiteles értéknyilvántartóként elfogadott főkönyvet, a blokkláncot egy apró szeletében megváltoztassuk.

Való igaz, hogy a címek és a hozzájuk tartozó privát kulcsok alapesetben a bitcoinkliens által létrehozott fájlban tárolódnak a létrehozó személy számítógépén, amelyet tárcának *(wallet)* nevezünk. Azonban mivel a privát kulcs egy egyszerű karaktersor, így a fájlból kinyerhető és bármilyen egyéb formában is tárolható (akár egy papírlapra is felírható, vagy egyszerűen meg is tanulható), és emiatt semmiképpen sem definiálhatjuk elektronikus adatként. Az elektronikus tárolás csupán egy lehetőség a számtalan tárolási mód közül – éppúgy, mint bármilyen adat esetében.

17 Lásd például *„A bitcoinok számítógépes fájlok, hasonlóan egy szöveges vagy mp3 fájlhoz, és éppúgy megsemmisíthetők vagy elveszthetők, mint a papírpénz."* M. Nikolei Kaplanov: Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. 25 Loyola Consumer Law Review, vol. 25, iss. 1, 2012, p. 116.

18 Florian Tschorsch – Björn Scheuermann: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys & Tutorials, vol. 18, iss. 3, 2016, p. 2088.

19 Szándékosan nem a „jogosultság" szót használom, ugyanis a blokkláncnak édesmindegy, hogy valaki jogosan, vagy adott esetben teljesen jogtalanul jutott hozzá egy privát kulcshoz.

20 A bitcoinhasználók száma – a rendszer anonimitásából és azon tényből kifolyólag, hogy bárki bármennyi címet használhat – nem határozható meg pontosan, azonban nagyságrendjük megbecsülhető. Lásd például How Many People Use Bitcoin? https://www.bitcoinmarketjournal.com/how-many-people-use-bitcoin/

Fontos megjegyezni továbbá, hogy a címek és a hozzájuk tartozó privát kulcsok egymással matematikai összefüggésben állnak: a privát kulcsból bármikor egy pillanat alatt kiszámolható a cím.[21] A címet jelentő karaktersor tárolása így nem is feltétlenül szükséges, illetve olyan sem fordulhat elő, hogy „elveszítjük" a privát kulcsunkhoz tartozó címet. Fordítva ez természetesen nem igaz; a címből nem számolható ki a privát kulcs, hiszen akkor bárki bármilyen címről szabadon utalhatna. Ennek tudatában tehát fokozottan is igaz, hogy a bitcoin birtoklása csupán a privát kulcs ismereteként definiálható.

A kriptovaluták tárolóeszközként történő használata

A kriptovaluták már részletezett tulajdonságai tökéletesen alkalmassá teszik őket bármilyen vagyoni érték elrejtésére, ezért a bűncselekményből származó vagyon kriptovaluták útján történő tárolása a bűnözők által is előszeretettel alkalmazott módszer.

A gyakorlati munka során gyakran szembesülünk azzal, hogy a bűnelkövetők az általuk elkövetett – bármilyen – bűncselekményből származó vagyont igyekeznek mielőbb bitcoinra váltani. Minderre az elkövetőknek jó okuk van, hiszen – mint említettem – ez után már csak arra kell figyelmet fordítaniuk, hogy a címhez tartozó privát kulcsot megőrizzék.

A privát kulcs nem más, mint egy 51 karakter (és ebben az esetben 5-ös számmal kezdődik), vagy pedig egy 52 karakter (ebben az esetben pedig az első karakter L vagy K betű) hosszúságú karaktersor, ami a következőképpen nézhet ki (bitcoin esetén):

5K9sk2YjAhA6Vvcah7oJJJenpB3SeTn9cUepihCj2GWrKwZrztE.

A bitcoincímek ezzel szemben 26–35 karakter hosszúságúak, és 1-es számmal, 3-as számmal, vagy pedig „bc1" karaktersorral kezdődhetnek. A fenti privát kulcshoz tartozó cím a következő[22]:

1C4TAcm5AADfomDCGhbssUajm5F2wjTatP.

21 A rendszer itt is hash függvényeket használ.

22 A különböző formátumok oka, hogy az ilyen címek részben különböző tulajdonságúak (például beállítható, hogy egy címhez való hozzáféréshez egyszerre több kulcs ismeretére legyen szükség), vagy pedig a bitcoinprotokoll újabb verziói alatt készültek. Ennek mélyebb technikai ismerete a jelen téma szempontjából nem fontos.

Mint már említettem, a privát kulcsból a cím bármely klienssel kiszámolható, így annak megőrzése nem is feltétlenül szükséges. Megjegyzendő továbbá, hogy más kriptovaluták esetén a címek és privát kulcsok formátuma is más, azonban ezek jellemzői is minden nehézség nélkül kideríthetők.

Alapvetően – ha az elkövető bitcoinklienst használ a cím generálásához – a privát kulcs egy fájlban tárolódik a program által létrehozott mappában (a fájl neve kliensenként eltérő, azonban általában tartalmazza a „wallet" megnevezést, a kiterjesztése pedig „.dat", ami az egyszerű adatfájlokhoz tartozó legáltalánosabb kiterjesztés).[23] Ez után a tulajdonosa a fájlt külső adathordozóra mentheti, feltöltheti egy felhőbe, vagy bármilyen egyéb módon tárolhatja, ami elektronikus adatok tárolása esetén felvetődhet. Természetesen annak sincs akadálya, hogy a fájlt bármilyen erre szolgáló programmal titkosítsa, így pedig az elrejtésével sem kell bajlódnia, hiszen elég csupán megjegyeznie a jelszót.

Léteznek továbbá olyan titkosító eszközök – kriptográfiai algoritmusokat használó hardverkulcsok –, amelyek lehetővé teszik, hogy egy adott címről csak a hardverkulcs birtokában lehessen elutalni az összeget. A hardverkulcsot (amely egy pendrive-ra hasonlít) ilyenkor csatlakoztatni kell a számítógéphez, ugyanis a privát kulcsot a megfelelő kliens csak a hardverkulcson tárolt adatok birtokában képes kiszámolni (ezek az adatok a hardverkulcsból semmilyen módon nem nyerhetők ki). Mindez azt jelenti, hogy a cím felett csak az rendelkezhet, akinek ténylegesen is a birtokában van egy ilyen kulcs.

Az előbbi esetekben azonban az elkövetőnek vállalnia kell annak a kockázatát, hogy ha a fájlt tartalmazó összes adathordozó vagy a hardverkulcs megsemmisül, akkor elveszti a hozzáférést a kriptovalutához. Ennek kiküszöbölése érdekében megteheti, hogy a fájlból egyszerűen kinyeri a privát kulcsot, majd azt kinyomtatja, vagy más – nem elektronikus – adathordozón tárolja. Ha a kriptovalutát később el szeretné költeni, nincs más dolga, mint bármelyik kliensbe újra begépelni a privát kulcsot.

Utóbbi módszerrel azonban azt kockáztatja a tulajdonos, hogy a privát kulcsot más is megismerheti, hiszen elég, ha az adathordozóról akár csak egy fényképet készít (nem beszélve arról, hogy az adathordozó természetesen ebben az esetben is megsemmisülhet vagy elveszhet).

A legbiztosabb módja tehát a bitcoin tárolásának, ha valaki megjegyzi a privát kulcsot, majd pedig törli azt minden olyan adathordozóról, amely va-

23 Szigorúan véve ezt a fájlt nevezzük tárcának, ami tehát több címet is tartalmazhat (és általában tartalmaz is). A köznyelvben azonban gyakran – pontatlanul – magára a címre is tárcaként hivatkoznak, illetve az online szolgáltatóknál létrehozott fiókokat is tárcának nevezik.

laha tartalmazta. Ily módon a privát kulcs csak a bitcoin tulajdonosának tudatában létezik, és azt tőle megszerezni semmilyen módon nem lehet (ha csak ő maga el nem árulja). Természetesen egy privát kulcsot megjegyezni – ha nem is lehetetlen, ám nyilvánvalóan – nem egyszerű feladat, és az sem zárható ki, hogy valaki több év után elfelejti a pontos karaktereket. Már pedig egyetlen karakterben való tévedés is használhatatlanná teszi a kulcsot.

Mivel azonban a privát kulcs lényegében nem más, mint egy matematikai függvény eredménye, így bármilyen adatból képezhető. Mindez azt jelenti, hogy bármilyen értelmes szóból vagy mondatból is generálható privát kulcs, és ebben az esetben csupán ennek a megjegyzése szükséges.[24] Mivel egy függvény azonos bemeneti érték esetén mindig ugyanazt az eredményt adja, így a privát kulcs bármikor újragenerálható a szó ismeretében.[25]

A példaként mutatott privát kulcsot és címet a Nemzeti Közszolgálati Egyetem kifejezésből számítottam ki, így ha erre a címre utalnék bitcoint, elég lenne ennek a tényét megjegyeznem az örök időkig tartó birtoklásához. Természetesen ez azzal a kockázattal jár, hogy ha másnak is eszébe jut ugyanebből a kifejezésből privát kulcsot generálni, akkor ő is elköltheti a címen lévő bitcoint.[26] Mindazonáltal könnyű belátni, hogy megfelelő bonyolultságú kifejezés használata esetén igen kevés esély van arra, hogy más is éppen ugyanazt a kifejezést választja majd. Az ilyen típusú tárolást a köznyelvben *brain wallet*nek hívják (a kifejezés az agy és tárca szavakból áll, magyar megfelelője nincs).

Könnyen belátható, hogy ha az elkövető *brain wallet*et használ, akkor egy házkutatás nyilvánvalóan nem vezethet semmiféle eredményre, hiszen csupán az emberi tudatban létező információt semmilyen kényszerintézkedéssel nem lehet megszerezni.

24 Nemcsak szavakból generálható természetesen privát kulcs, hanem más adatból is (így akár zenéből, képből, vagy bármilyen egyéb adatállományból), hiszen az informatika világában minden fájl lefordítható egyesek és nullák sorozatává. Ennek azonban sok gyakorlati haszna nincs (hiszen ilyen esetben a fájlt is meg kell őrizni).

25 Mivel matematikai műveletről van szó, mindez papírral és ceruzával is kiszámolható, azonban természetesen bármikor találhatók erre szolgáló programok és weboldalak az interneten (például https://www.bitaddress.org).

26 Ha megnézzük az 1-es számból generált címhez tartozó forgalmat a blokkláncon, láthatjuk, hogy az évek során több mint ezer tranzakció kapcsán volt érintett ez a cím. Nyilvánvalóan ennek az oka, hogy a bitcoint használók millióri közül egymástól függetlenül többnek is eszébe jutott az a „nagyszerű" ötlet, hogy az 1-es számból generáljon magának bitcoincímet. Ha valaki türelmesen figyelné a fenti cím forgalmát, akkor a következő utalásnál az érkező bitcoint minden további nélkül továbbutalhatná magának.

Kimondhatjuk tehát, hogy a bitcoinnal létrejött az emberi történelem során az első olyan vagyontárolási mód, amikor is egy információ önmagában – a materiális világban megjelenő minden más dolog közrehatása nélkül – értékkel bír.

Leginkább csak ahhoz hasonlítható ez, mint amikor elásunk egy láda kincset, aminek egyedül mi ismerjük a helyét; viszont az információ értékét végső soron ebben az esetben is a kincs biztosítja, ez pedig elenyészhet, vagy megtalálhatja más. A bitcoin esetén a „kincs" a blokklánc, ami viszont elenyészni nem fog (hiszen a csomópontok képében minden pillanatban egyszerre tízezer helyen van jelen a világon, és ez a szám csak egyre nő), illetve „megtalálni" sem fogja más (ugyanis a privát kulcs címből való kiszámítása gyakorlatilag lehetetlen[27]). Mindemellett a kincsesládánkhoz csupán azon az egy helyen férhetünk újra hozzá, ahol azt elrejtettük, míg a blokklánchoz történő hozzáférés a világ bármely pontjáról lehetséges, ahol van internetkapcsolat.

Mindez azt is jelenti, hogy ha az elkövető a *brain wallet* létrehozása során nem követ el olyan hibát, ami által a privát kulcs napvilágra kerülne, akkor a nyomozó hatóság a bitcoin (vagy más kriptovaluta) megszerzése érdekében semmit sem tehet. Ilyen módon a bűnöző a bűncselekményt követően minden további nélkül megvárhatja akár azt is, hogy a cselekménye elévüljön (vagy ha elfogták, a büntetése leteljen), majd nyugodtan elköltheti az így tárolt vagyont. Mindezen idő alatt pedig a bűncselekményből származó vagyon pontos helye mindenki számára látható lesz a blokkláncon, azonban ahhoz hozzáférni senki sem tud.

Az említett körülmények egyértelműen olyan új helyzet elé állíthatják majd a nyomozó hatóságokat, amire korábban sosem volt példa a büntetőeljárások során.

A bitcoin lefoglalása

A következőkben az kívánom bemutatni, hogy ha az eljárás folyamán bármely okból szükségessé válik az elkövető birtokában lévő bitcoin lefoglalása, akkor ez milyen gyakorlati lépések alapján tehető meg. Bár a címben csupán a lefoglalásról teszek említést, természetesen az elképzelt szituáció egy házkutatással egybekötött lefoglalásra vonatkozik, nem pedig arra az esetre, ha az elkövető önként „adná át" a nyomozó hatóság tagjának a kriptovalutát.

27 Ignacio Mas – David Lee Kuo Chuen: Bitcoin Like Protocols and Innovations. David Lee Kuo Chuen (ed.): Handbook of Digital Currency. Academic Press, 2015, p. 420.

Ennek okán a lépések részletezésekor kitérek a házkutatáskor szem előtt tartandó elvekre is.

Végül fel kívánom hívni a figyelmet arra, hogy álláspontom szerint a bitcoin megfelelő tárolásához a nyomozó hatóság részéről központi szintű lépések meghozatalára – egészen pontosan egy megfelelően beállított hatósági tárca létrehozatalára – van szükség, ez azonban csupán hosszabb folyamat eredménye lehet. A lefoglalás azonban nyilvánvalóan nem képzelhető el anélkül, hogy a lefoglalt bitcoint valamilyen módon ne tárolnánk. A lefoglalás lépéseit leíró részt ezért olyan szellemben készítettem el, hogy annak alkalmazásával egy nyomozó akár már holnap képes legyen bitcoint lefoglalni, és a *körülményekhez képest* megfelelően tárolni. Optimálisnak viszont értelemszerűen azt tartanám, ha egy jövőbeli időpontban megvalósulnának a tárolás kapcsán általam indokoltnak vélt lépések, és onnantól fogva a nyomozás során lefoglalt bitcoin egy központi tárcába kerülne.

A bitcoin lefoglalásának lépései

Az eddig kifejtettek alapján nyilvánvaló, hogy bitcoin esetében zár alá vételnek és hasonló jellegű intézkedéseknek még elméletben sincs értelme, ugyanis nincs semmilyen szerv, amely végrehajthatná a hatóság határozatát. 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.

A következőkben összefoglalom azokat a főbb lépéseket, amelyeket a nyomozó hatóság tagjának ezen eljárás során ajánlatos végrehajtania. Annak érdekében, hogy mindez valóban alkalmazható is legyen a gyakorlatban, a lépéseket nem csupán elméleti jelleggel, hanem egy konkrét bitcoinkliens alkalmazásán keresztül mutatom be.

Megismételvén a korábban elmondottakat: ha a hatóságnak már a rendelkezésére áll egy központi cím, akkor a lefoglaláshoz szükséges cím létrehozására vonatkozó lépések értelemszerűen kihagyhatók.

A lefoglalás – a tranzakció kikényszerítése – a következő nyolc lépésben hajtható végre. Az első három lépés a lefoglalás előkészületének, míg a többi a tényleges végrehajtásának tekinthető.

– A tranzakcióhoz szükséges számítógép előkészítése.
– A fogadásra szolgáló cím elkészítése.
– A fogadásra szolgáló címhez tartozó privát kulcs biztonságba helyezése.

– A lefoglalást szenvedő privát kulcsának felkutatása.
– A privát kulcsok kinyerése a tárcából.
– A privát kulcsok importálása a tranzakcióhoz használandó számítógépre.
– A tranzakció végrehajtása.
– A tranzakció ellenőrzése.

A tranzakcióhoz szükséges számítógép előkészítése

Az első lépésben elő kell készítenünk egy olyan hordozható, internetkapcsolattal bíró számítógépet, amellyel a kikényszerített utalást végre fogjuk tudni hajtani a helyszínen.

Bár a tranzakció elvileg végrehajtható az eljárás alá vont számítógépének használatával is, azonban ez könnyen akadályokba ütközhet. Elképzelhető, hogy a kérdéses számítógépen nincs internetkapcsolat, vagy jelszóval védett bitcoinklienst telepítettek rá, esetleg a privát kulcsra végül csupán egy egyszerű szöveges fájlban vagy egy papírlapon rögzítve bukkanunk. Utóbbi esetekben nem is áll majd rendelkezésünkre megfelelő kliens vagy számítógép.

Az előkészítés során telepíteni kell egy bitcoinklienst a használni kívánt számítógépre. Bár ebből többfajta is létezik, azonban a lefoglalás szempontjából megfelelő kliensnek jellemző tulajdonságai kell hogy legyenek.

A kliensnek értelemszerűen ismernie kell a teljes blokkláncot, hiszen máskülönben nem tudná ellenőrizni a tranzakciók hitelességét. A teljes blokklánc mérete azonban több száz gigabyte – ami természetesen folyamatosan növekszik –, így letöltése egyrészről hosszabb ideig is eltarthat, másrészről pedig minden indításnál újabb frissítésre van szükség. E problémák kiküszöbölése érdekében ajánlatos olyan klienst használni, amely nem tölti le a teljes blokkláncot, hanem annak adatait egy olyan távoli szerver útján ellenőrzi, amelyen az már rendelkezésre áll. Mindemellett természetesen a kliensnek megbízható forrásból is kell származnia, máskülönben akár adathalász vírust is tartalmazhat.

Az említett feltételeknek megfelelő kliensnek tekinthető az Electrum, amely a https://electrum.org/#download címen érhető el. Az említett címen az Electrum több verziója is megtalálható. Ezek közül – feltételezve természetesen, hogy Windowst használunk – a *Portable version* használható a legegyszerűbben, ugyanis ez nem igényel semmiféle telepítést.

A letöltés után a programban létre kell majd hoznunk egy tárcát, amelybe később a lefoglalást szenvedőtől megszerzett privát kulcsokat importáljuk a tranzakció végrehajtásához (ezt részletesen *A tranzakció végrehajtása* alcím

alatti részben mutatom be). A lefoglaláshoz azonban egy másik számítógépen létre kell hoznunk egy másik tárcát is, amelyben majd az utalás fogadásához szükséges címet generáljuk. Mivel mindkét tárca létrehozásának lépései azonosak, ezért ezt csupán egyszer (e második tárca kapcsán) mutatom be a következő pontokban.

A fogadásra szolgáló cím elkészítése

A lefoglaláshoz tehát létre kell hoznunk egy másik tárcát is, amely majd tartalmazza azt a hatósági címet, amelyre a lefoglalandó bitcoint utalni szándékozunk. Bár ilyen címet az előző pontban említett tárcával együtt is létrehozhatnánk, biztonsági megfontolásból azonban ez mégsem indokolt.

A tranzakció végrehajtásához mindenképpen internetkapcsolatra van ugyanis szükség, így ha a hatósági címhez szükséges tárcát ugyanazon a számítógépen készítenénk el, fennállna a veszélye, hogy a számítógépen lévő esetleges adathalász vírusok az újonnan létrehozott privát kulcsokat megszerzik.[28]

Az előbbiek kizárása érdekében a bitcoinklienst fel kell telepíteni egy internetre nem rákötött számítógépre is, és a bitcoinok fogadására szolgáló tárcát ezen kell létrehozni.

A tárcában lévő címek és a hozzájuk tartozó privát kulcsok elkészítéséhez nincs szükség internetkapcsolatra, hiszen ezek csupán matematikai műveletek eredményei. Az így alkotott címek természetesen nem is fognak megjelenni a blokkláncban mindaddig, amíg egy tranzakció során nem adjuk meg azokat az utalás céljaként. Bár elviekben akár előfordulhatna, hogy időközben véletlenül valaki más is ugyanazt a címet generálja magának, ám a karaktersor bonyolultsága miatt ez gyakorlatilag kizárt, a lehetséges bitcoincímek száma 2^{160} lehet.[29] Azonban ezzel együtt is, a blokkláncot nyilvántartó oldalakon[30] közvetlenül a tranzakció megkezdése előtt bármikor ellenőrizhetjük, hogy az adott cím nem szerepel-e már véletlenül a blokkláncban.

Ha az eljárás későbbi szakaszában a lefoglalt bitcoint tovább kell utalnunk – vagy a lefoglalás megszüntetése miatt, vagy mert az eljárás befejeztével az állam tulajdonába kerül és értékesíteni kell –, akkor a tárcát elég csupán közvetlenül az utalás előtt online számítógépre másolnunk.

28 Ennek lehetősége ugyanis sosem zárható ki teljesen egy internetkapcsolattal bíró számítógépen.

29 Ez azt jelenti, hogy ha egymilliárd ember használna a földön bitcoint, és mindegyik tíz címet generálna, két cím egyezésének az esélye akkor is csak 0.00000000000000000000000000000000000007 százalék lenne.

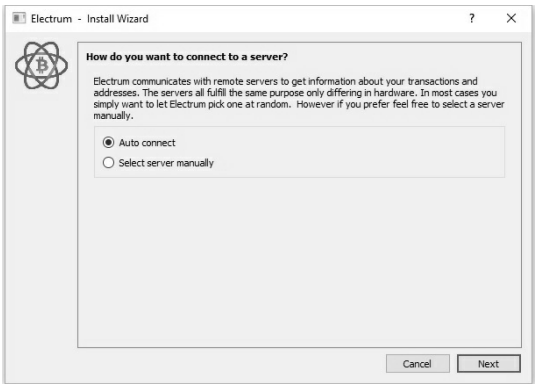
30 Mint például a https://blockchain.info/

Nyilvánvalóan célszerű minden lefoglalást szenvedő esetén külön címet generálni, azonban a címek számát egyéb célszerűségi okok is meghatározhatják (külön címek a külön bűncselekményekből származó bitcoinok biztosítására stb.).

A tárca létrehozásának lépései a következők.

Az első indítás után be kell állítanunk, hogy a kliens milyen módon csatlakozzon a blokkláncot tartalmazó szerverhez. A beállítást hagyjuk az alapértelmezettként felajánlott *Auto connect* lehetőségen, majd kattintsunk a *Next* fülre! *(1. számú ábra)*

1. számú ábra



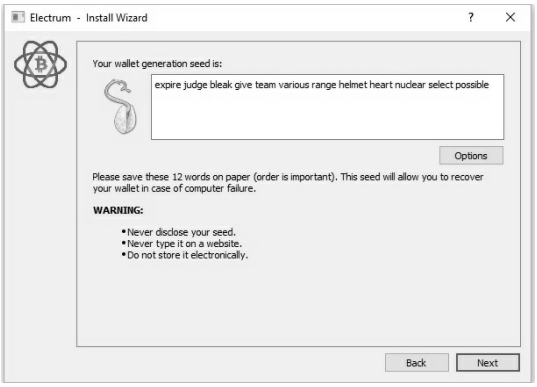
Ezt követően a kliens létrehoz egy *electrumdata* elnevezésű mappát ugyanazon a helyen, ahonnan a letöltött klienst elindítottuk. Ez a mappa fogja tartalmazni a *wallets* almappában *defaultwallet* néven a létrehozott tárcafájlt (ha csak nem változtatjuk meg a tárca nevét a következő ablakban).

Az ez után felugró három fülben a felajánlott lehetőségek közül sorban válasszuk ki a *Standard wallet, Create new seed, Standard* opciókat, hogy a következő ablakhoz jussunk.

Az előbbi ablakban a program egy *seed*nek (magnak) nevezett, 12 véletlenszerű szóból álló listát fog feltüntetni, amit fel kell jegyeznünk, és a következő ablakban ugyanilyen formában kell majd megadnunk. *(2. számú ábra)*

Ez egy biztonsági megoldás, ugyanis a *seed* ismeretében (ami gyakorlatilag egy kriptográfiai művelet alapjaként szolgál) később bármikor visszaállíthatnánk a tárcában lévő összes címet és privát kulcsot, ha valamilyen okból elvesztenénk azokat.

2. számú ábra



Minderre a jelen eljárási rendben nem lesz szükségünk, az opció azonban sajnos nem kerülhető meg. Másoljuk tehát ki a szavakat, majd a következő ablakban adjuk meg őket újból.

Ha ezt megtettük, a kliens fel fogja ajánlani, hogy készítsünk jelszót is a tárcához. Ha állítanánk be jelszót, az a privát kulcsok kliensen belüli megjelenítéséhez és ezáltal az utalások végrehajtásához lenne szükséges. Mivel azonban a tárcát – mint azt a későbbiekben kifejtem – a lefoglalás után a programból törölni fogjuk, így e biztonsági lépcső közbeiktatása felesleges.

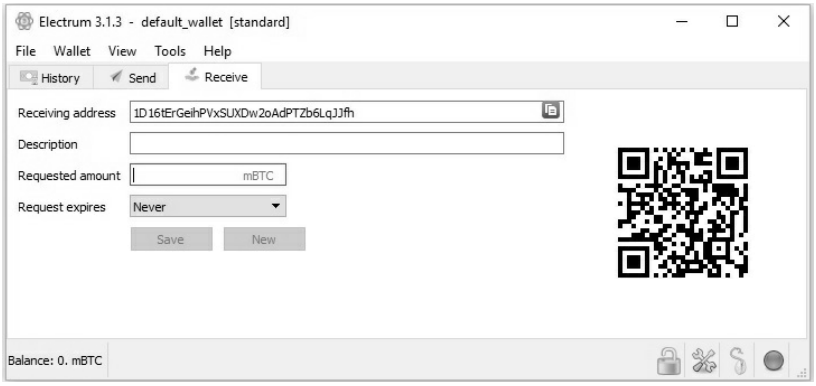
A mezőket üresen hagyva lépjünk tehát tovább, majd hasonló megfontolásból a *seed*ről készült előző feljegyzésünket is semmisítsük meg (arra a továbbiakban nem lesz szükségünk, ha azonban illetéktelen kezekbe kerülne, akkor a tárca újragenerálásával a lefoglalt bitcoinhoz más is hozzáférhetne).

Az előbbiek után a program létrehoz egy tárcát, amelybe belépve a *Receive* fül alatt láthatjuk is az első címünket a hozzá tartozó QR-kóddal.[31] *(3. számú ábra)*

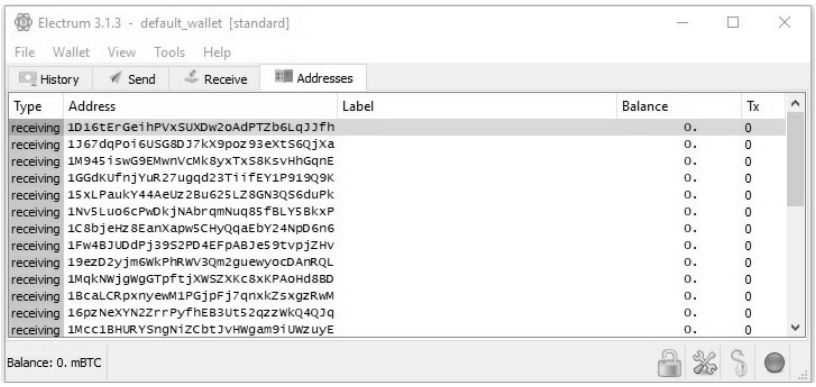
A tárcában azonban valójában ezzel egyidejűleg több cím létrehozására is sor kerül, amelyeket a *View* és a *Show Addresses* opciókra kattintva, majd pedig a megjelenő *Addresses* fülre lépve láthatunk. A *Balance* oszlop jelöli az adott címekhez tartozó bitcoin mennyiségét, amely jelen esetben mindenhol nulla. *(4. számú ábra)*

31 A QR-kódok lényege, hogy hosszabb szövegeket (mint amilyen egy bitcoincím is) grafikus formában tárolnak, így a megfelelő applikációkkal olvasva őket nem kell begépelni vagy átmásolni az adott szöveget. A mobilra letölthető tárcák legtöbbje képes QR-kódot beolvasni, így ez kényelmi funkciónak tekinthető.

3. számú ábra



4. számú ábra



A következő lépésben a szükséges mennyiségű címet egy külső adathordozó segítségével át kell másolnunk a tranzakcióhoz előkészített gépre, hogy a lefoglalás előtt majd célként meg tudjuk adni a kliensben. Bár a címet le is gépelhetjük, célszerű másolást alkalmazni, ugyanis bármely karakter elütése esetén a tranzakció nem jön létre (a karaktersor egyaránt tartalmaz kis- és nagybetűket, illetve számokat).

A címekhez tartozó privát kulcsokat természetesen nem kell átmásolnunk a másik számítógépre, ugyanis a bitcoin fogadásához azokra nincs szükségünk.

Jobb gombbal valamelyik címre kattintva, a *Copy Address* paranccsal másoljuk vágólapra bármelyik általunk választott címet, ezt követően illesszük azt egy egyszerű szöveges fájlba, és egy – lehetőleg előzőleg formatált – pendrive segítségével másoljuk át a tranzakcióhoz használandó számítógépre.

A fogadó címhez tartozó privát kulcs biztonságba helyezése

A tárca létrehozása után digitális mentést fogunk készíteni az előző pontban kimásolt címekhez tartozó privát kulcsokról. *(5. számú ábra)*

5. számú ábra

A privát kulcsot az adott címre jobb gombbal kattintva a *Private Key* parancscsal jeleníthetjük meg (mint korábban említettem, a privát kulcs jelen esetben az L karakterrel kezdődik, a „p2pkh" csupán a kulcs létrehozása során alkalmazott script típusát jelöli, ami esetünkben irreleváns).

Mind a címet – az előző pontban kifejtettek szerint –, mind a hozzá tartozó privát kulcsot másoljuk át egy egyszerű szöveges fájlba, amit ezt követően másoljunk külső adathordozóra (valamilyen optikai lemez használata javasolt).[32] A fájlt indokolt továbbá jelszóval is védeni, amelynek legegyszerűbb módja annak tömörítése WinRAR-ral, jelszó megadása mellett (természetesen még a lemezre másolás előtt).

A jelszót természetesen szintén úgy kell tárolnunk, hogy illetéktelen személy azt ne ismerhesse meg. Erre megfelelő módszer lehet, ha azt – annak érdekében, hogy átvilágítással se lehessen kifürkészni – egy kartonlapra írva, zárt borítékban tároljuk az adathordozótól elkülönítve.

Az adathordozót a bűnjelekhez hasonlóan kell csomagolnunk szintén olyan módon, hogy a bűnjelzacskó felnyitása állagsérelem okozása nélkül ne legyen lehetséges. Az adathordozót ez után elhelyezhetjük a bűnjelkamrában, míg a jelszót az eljárás során egy másik helyiségben indokolt őrizni.

32 Bár a címek a hozzájuk tartozó privát kulcsokból visszafejthetők ugyan, praktikus okokból azonban indokolt azokat is a privát kulcsok mellett feltüntetni.

Az adathordozó tárolásánál figyelemmel kell lennünk arra is, hogy megsemmisülése vagy elvesztése esetén végleg elveszítjük a lefoglalt bitcoin feletti rendelkezés lehetőségét, ajánlott ezért egyidejűleg egy biztonsági másolatot is létrehozni (és hasonló módon tárolni).

A mentések elkészítése után a tárcafájlt (ami a már említett mappában található *defaultwallet* néven) törölnünk kell a létrehozáshoz használt számítógépről, hogy később senkinek se legyen módja megismerni a privát kulcsokat. Ügyeljünk arra, hogy az adatokat végleg töröljük a merevlemezről, hogy azok erre szolgáló programok segítségével se legyenek visszaállíthatók. Ilyen célra egyszerűen és ingyen használható a File Shredder nevű alkalmazás.[33]

A lefoglalást szenvedő privát kulcsának felkutatása

A házkutatás megkezdése előtt mindenképpen indokolt adatgyűjtést folytatnunk arra vonatkozóan, hogy a célszemély milyen módon tárolhatja az eljárás tárgyát képező bitcoint. Ehhez vegyük igénybe blokklánc segítségét is, ugyanis könnyen kiderülhet, hogy a keresett bitcoint elutalták egy online tőzsdéhez, pénztárca-szolgáltatóhoz, vagy egyéb más szolgáltatóhoz (ezek címei általában egyszerű Google-keresés alapján is azonosíthatók). Különösen árulkodó lehet, ha az adott címen nagy összegű bitcoin fordult meg, vagy rendkívül gyakoriak az utalások. Ilyen esetben máris tudhatjuk, hogy a házkutatás során nem a privát kulcsok, hanem az e szolgáltatókhoz tartozó bejelentkezési adatok felkutatása lesz a fő cél (természetesen ilyen esetben az utalást is e szolgáltatók felületén kell majd végrehajtanunk).
Ha nem találtunk olyan adatokat, amelyek az inkriminált címre vonatkozóan különösebb iránymutatással szolgálnának, vagy egyáltalán nem is ismerünk címet, akkor a házkutatás során kell a privát kulcsokra utaló nyomokat felkutatnunk.

A házkutatás megkezdésekor arra kell törekednünk tehát, hogy az eljárás alá vont a számítógépét ne tudja a kényszerintézkedés megkezdése után kikapcsolni. Ajánlott természetesen a házkutatást is olyan időpontban foganatosítani, amikor feltételezzük, hogy a számítógépet bekapcsolt állapotban találhatjuk (nem indokolt tehát ilyen esetben a hajnali órákban kopogtatni, célszerűbb abban az időszakban felkeresni az eljárás alá vontat, amikor délutáni vagy esti pihenését tölti).

33 http://www.fileshredder.org/

Az adatok lefoglalására irányuló házkutatások során általában a nyomozó hatóság igyekszik lefoglalni a helyszínen talált eszközöket, amelyekről aztán a lefoglalás után mentést készít az adattartalom későbbi vizsgálata céljából.

Hogyha azonban a kényszerintézkedés bitcoin felkutatására irányul, akkor az effajta késlekedésre nincs mód; a megtalált elektronikai eszközöket a helyszínen kell átvizsgálni addig, míg lehetőségünk van az eljárás alá vont személyt felügyelet alatt tartani. Máskülönben a távozásunk után azonnal lehetősége nyílna más címre utalni a bűncselekmény tárgyát képező bitcoint, még ha egyébként a privát kulcsok megtalálhatók lettek volna később a lefoglalt eszközökön is.

Ha sikerült a számítógépet bekapcsolt állapotban találnunk (vagy az nem volt jelszóval védve), akkor tehát azonnal meg kell kezdenünk felkutatni a számítógépen lévő klienseket (alapértelmezés szerint ugyanis a tárcafájlok általában e programok gyökérkönyvtárában találhatók). A kliensek felkutatása azért is indokolt, mert a tárcából a privát kulcsok kinyerése legkönnyebben a lefoglalást szenvedő által használt programmal lehetséges. Bár az Electrum képes lehet a más típusú kliensek által létrehozott tárcafájlokat is megnyitni, azonban könnyen felléphetnek kompatibilitási problémák is. A tárcafájlok pontos helye felkutatásának megkönnyítése érdekében végezhetünk internetes keresést is, ez alapján ugyanis gyorsan megállapíthatjuk, hogy egy-egy adott kliensnek mi az alapértelmezett mentési helye és tárcaneve. Hogyha a számítógépen nem találunk bitcoinklienst, akkor a meghajtókon egyszerű keresést kell végeznünk a *„wallet, private key, seed”* és egyéb olyan szótöredékekre, amelyekről feltételezzük, hogy a privát kulcsokhoz vezethetnek minket.

A meghajtók tartalmának átvizsgálása mellett ellenőriznünk kell a böngészési előzményeket és könyvjelzőket is. Ennek során akkor is fel kell jegyeznünk az előzményekben talált váltókat és egyéb szolgáltatókat, ha hozzájuk bejelentkezési adatokat nem sikerült megállapítanunk, ugyanis az eljárás későbbi szakaszában megkeresést küldhetünk részükre a célszemélyre vonatkozóan. Ugyanez vonatkozik a felhőszolgáltatókra is, ugyanis a privát kulcsok náluk is tárolhatók. A böngészési előzmények mellett érdemes ellenőriznünk továbbá a sütiket is, ugyanis ezeket a felhasználók – az előzményekkel ellentétben – hajlamosak nem törölni.

A számítógépek mellett természetesen – ugyanilyen elvek alapján – ellenőriznünk kell a célszemély birtokában lévő összes egyéb elektronikai eszközt is (tabletek, mobiltelefonok), az ilyen eszközökön szokásos tárcák után kutatva.

Természetesen lehetséges, hogy az eljárás alanya papír alapon, vagy más külső adathordozón tárolja a privát kulcsokat, így nem csupán a számítógépeket, telefonokat (stb.) kell felkutatnunk. Az elektronikus és hagyományos iratok átvizsgálása során figyelemmel kell lennünk az olyan iratokra is, amelyek egymástól független szavakat tartalmaznak, ugyanis nem kizárt, hogy a célszemély feljegyzést készített a tárcájához tartozó *seed*ről. Ha nem bitcoint keresünk, akkor még a házkutatás előtt érdemes tájékozódni afelől, hogy az adott kriptovaluta privát kulcsai milyen formátummal bírnak.

Szintén figyelemmel kell lenni a QR-kódokat tartalmazó iratokra is, ugyanis ezek is jó eséllyel takarhatnak bitcoin címeket éppúgy, mint hozzájuk tartozó privát kulcsokat. Ne feledkezzünk meg továbbá a hardverkulcsok felkutatásáról sem, ha feltételezzük, hogy a gyanúsított ilyet használt a bitcoinjai megőrzése érdekében (tartsuk szem előtt azonban, hogy ezen eszközök PIN-kóddal is elláthatók).

A manapság legelterjedtebb hardverkulcsok a *6. számú ábrá*n láthatók:

6. számú ábra

A *7. számú ábrá*n láthatóhoz hasonló, papíralapú tárcát kell keresnünk jellemzően abban az esetben, amikor az alany ATM-en keresztül vásárolt bitcoint (új tárca létrehozása esetén az ATM-ek ugyanis kinyomtatnak egy címet és privát kulcsot is tartalmazó papírtárcát). Az erre vonatkozó információk felderítése során szintén igénybe vehetjük a blokkláncot, ugyanis az ATM-ek címe is legtöbbször ismert.

Amennyiben a helyszínen nem voltunk képesek felkutatni a privát kulcsot, még nem tekinthetünk el automatikusan az eszközök lefoglalásától, ugyanis lehet még esélyünk azok megtalálására a benti, alaposabb vizsgálat során is. Természetesen éppúgy bízhatunk abban is, hogy az elkövetőnek nincs másolata a privát kulcsairól (így a lefoglalás esetén sem fogja tudni a bitcoint továbbutalni), mint ahogy egyébként tartanunk kell tőle, hogy igen.

7. számú ábra

Az is előfordulhat továbbá, hogy egy nyomozás során nem is számítunk arra, hogy a célszemély rendelkezik bitcoinnal, azonban a lefoglalt eszközei átvizsgálása során később mégis erre vonatkozó adatokat találunk (bitcoinkliens, elmentett privát kulcs stb.). Ha az eljárásban indokolt lehet az így talált bitcoin lefoglalása is (például a kár megtérülésének biztosítása érdekében), ezt szintén a lehető legrövidebb időn belül kell megtennünk.

Ilyen esetekben természetesen külön kell lefoglalnunk a később feltárt bitcoint – már csak a tranzakció pontos dokumentálása és a jogorvoslati jog biztosítása érdekében is –, a lefoglalást pedig indokolt egy szemle keretében végrehajtani. A szemlejegyzőkönyvben így – a lefoglalás mellett – dokumentálhatjuk azt is, hogy miként tekintettük át az adathordozót, ezt a korábbi kényszerintézkedés során miért nem végeztük el helyben (időhiány, az adatok nagy mennyisége stb.), és eközben hol és hogyan bukkantunk olyan adatokra (például privát kulcs, tárcafájl), amelyek felhasználásával a lefoglalást végrehajtjuk. Ebben az esetben természetesen elegendő, ha a szemlét és a lefoglalást hatósági tanú jelenlétében végezzük el, befejeztével pedig haladéktalanul értesítjük az érintett személyt, akit utólag nyilatkoztatunk a panasztételi szándékáról (hiszen, ha még a lefoglalás előtt értesítenénk, akkor ezzel esetleg lehetőséget adnánk neki a bitcoin továbbutalására).

A privát kulcsok kinyerése a tárcából

A privát kulcsok azonosítására a legegyszerűbb módszer, ha a tárcát az elkövető által használt programmal nyitjuk meg. Ebben az esetben láthatjuk az elkövető által létrehozott címeket és az azokon szereplő összegeket is. Ilyen

esetben a privát kulcsokat az erre szolgáló funkcióval – a tranzakcióhoz előkészített számítógépre történő másolás céljából – egy szöveges fájlba menthetjük. Bár minden program felépítése más, az Electrumhoz hasonlóan általában *Private key* elnevezésű gombot kell keresnünk a privát kulcs megjelenítéséhez (amennyiben nem boldogulunk, használjuk a program súgóját vagy keressünk rá az interneten a funkció előhívásának mikéntjére az adott kliensben).

Ha valamilyen okból a program segítségével nem sikerült megjelenítenünk a privát kulcsokat, vagy nem is találtunk erre szolgáló programot a gépen, különálló tárcafájlt vagy privát kulcsokat azonban igen, akkor egyszerűen ezeket másoljuk át a tranzakcióhoz előkészített számítógépre.

A privát kulcsok importálása a tranzakcióhoz használandó számítógépre

Természetesen ha a házkutatás során feltárt klienssel, vagy webes alkalmazással el tudjuk utalni a bitcoint a hatósági címre, akkor tegyük ezt meg. Hogyha azonban csak egy különálló tárcafafájlt vagy privátkulcsot találunk, vagy más okból nem tudjuk a tranzakciót végrehajtani (például a vizsgált eszköz nem csatlakozik az internethez), akkor az általunk ebből a célból előkészített számítógépet kell igénybe vennünk az utaláshoz.

Tárcafájl esetén a fájlt másoljuk a korábban említett *electrumdata\wallets* mappába, ami után jó eséllyel az Electrum felismeri majd és megjeleníti az abban szereplő címeket az *Addresses* fül alatt (ehhez nem árt újraindítanunk a programot, majd ezt követően a *File/Open* paranccsal megnyitni a tárcát).

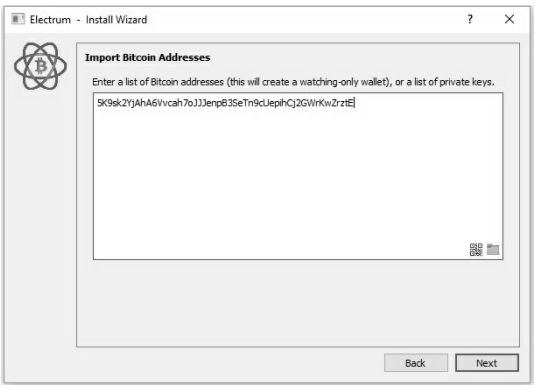
Ha ez után nem jelennek meg a tárcában lévő címek az *Addresses* fül alatt, akkor a tárcafájl nem kompatibilis az Electrum programmal. Ilyen esetben próbáljuk meg kideríteni, milyen programmal készült a tárcafájl, majd a letöltés és telepítés után nyerjük ki a privát kulcsokat *A privát kulcsok kinyerése a tárcából* című részben írtak szerint (ha a lefoglalást szenvedő nem hajlandó elárulni a kliens nevét, akkor erre vonatkozóan internetes kutatást végezhetünk a fájl elnevezése alapján, vagy megpróbálhatunk felkutatni telepítő fájlokat a számítógépen és a lomtárban).

Mielőtt azonban ezt megtennénk, kíséreljük meg egyszerűen Notepaddel is megnyitni a fájlt, ugyanis – egyszerű adatfájl lévén – jó eséllyel kaphatunk értelmezhető adatokat. Ha a privát kulcsot közvetlenül nem találjuk is meg így, lehet esélyünk akár a *seed* megismerésére, amit ezt követően csupán be kell emelnünk az Electrumba (a fogadásra szolgáló címek elkészítéséről szó-

ló pontban megismert lépések keretében) és ilyen módon újragenerálni a privát kulcsokat.

Ha csak különálló privát kulcsokat tudtunk felkutatni, akkor ezek importálására lesz szükség (ebben az esetben azonban már nem kell kompatibilitási problémáktól tartanunk). Ehhez a *File* legördülő menüben a *New/Restore* parancsra kattintva meg kell adnunk egy nevet az újonnan létrehozandó tárcának, majd ezt követően a fogadásra szolgáló címek létrehozása során már ismert ablakok tárulnak elénk. Most azonban a *Standard wallet* helyett az *Import bitcoin addresses or private keys* lehetőséget válasszuk. A megjelenő ablakban most a mag helyett a megszerzett privát kulcsokat kell az erre szolgáló mezőbe másolnunk. Egyszerre több privát kulcsot is megadhatunk, illetve a mező jobb alsó sarkában lévő mappa ikonra kattintva akár ki is jelölhetjük az általunk korábban létrehozott szöveges fájlt (a program automatikusan felismeri a benne lévő kulcsokat). Bár a program felajánlja, jelszót megint nem szükséges megadnunk.

8. számú ábra



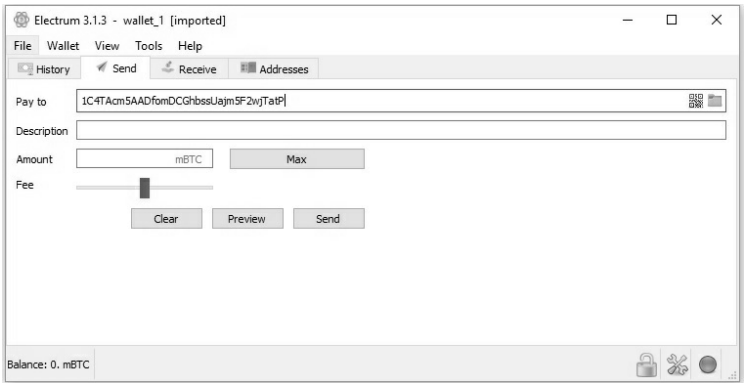
Ha a privát kulcsokat papír alapon találtuk meg, akkor kénytelenek vagyunk azokat manuálisan begépelni a fenti mezőbe. Ilyenkor különösen ügyeljünk a pontosságra, valamint a kis- és nagybetűk különbözőségére.

Az importálás után a kliens egy új tárcafájlt hoz létre, amely csak az importált címeket tartalmazza (ezek ekkor generálódnak a privát kulcsokból). Egy új Electrum-ablakban az *Addresses* fül alatt jelennek meg a címek, és az azokhoz rendelt bitcoinösszegek. A címre jobb gombbal kattintva, a *Private key* paranccsal akár meg is győződhetünk róla, hogy valóban az általunk korábban megadott privát kulcshoz tartozik a cím.

A tranzakció végrehajtása

A tranzakció végrehajtása előtt ellenőriznünk kell az internetkapcsolatot a tranzakcióhoz használt számítógépen, hiszen enélkül az utalás nem jöhet létre (a kapcsolat meglétét egyébként a kliens jobb alsó sarkában található zöld kör is jelzi). *(9. számú ábra)*

9. számú ábra



Ezt követően kattintsunk a *Send* fülre, majd a *Pay to* mezőbe a korábban létrehozott valamely hatósági címet másoljuk be. Ügyeljünk arra, hogy a karaktersort pontosan adjuk meg, hiszen ellenkező esetben nem jön létre a tranzakció. Az *Amount* mezőben kell megadnunk az elküldendő bitcoinösszeget.

Előfordulhat – sőt, valószínű –, hogy a lefoglalást szenvedő egyszerre több címen is tárol bitcoint. Ilyen esetben a tranzakció összegének az összes címen tárolt bitcoin együttes összegét adjuk meg, ha nincs különös indokunk a más-más címekre történő utalásra (mint tudjuk, egyszerre több címről is küldhetünk bitcoint egyetlen tranzakció során). A küldő címeket nem kell kijelölnünk, a program automatikusan levonja a rendelkezésre álló címekről a szükséges összeget. Természetesen összeadogatnunk sem kell az összegeket, elég, ha ehhez a *Max* gombra kattintunk (praktikus is ezt a módszert alkalmazni, hiszen így a félreszámolás veszélye nélkül „üríthetjük ki" egyszerre a lefoglalást szenvedő összes címét).

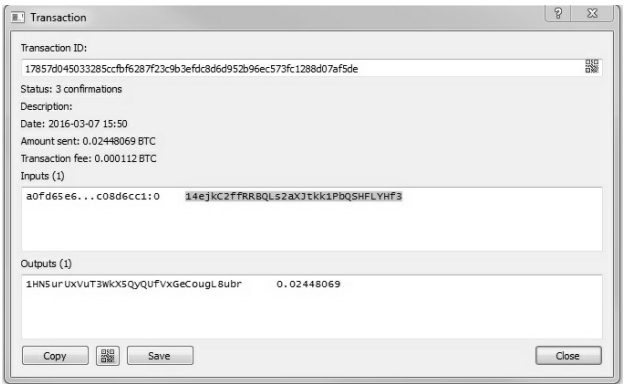
Az előbbi adatok megadása után kattintsunk a *Send* gombra (ha az Electrum nem ismerte fel a tárcafájlt és ezért kénytelenek voltunk az adott fájlnak megfelelő klienst letölteni, akkor természetesen a menüpontok eltérők lehetnek, azonban lényegében ugyanezen adatokat kell megadnunk).

A tranzakció végrehajtásához tranzakciós díjat kell fizetnünk, ez azonban elhanyagolható mértékű. Bár ennek összege hatással lehet a blokkba foglalás sebességére, ajánlott elfogadni az alapértelmezett mértéket (a tranzakciós díj nagyságát egyébiránt a *Tools/Preferences/Fees* menüpontban tudjuk módosítani).

A tranzakció ellenőrzése

A küldést követően néhány másodpercen belül megjelenik a *History* fül alatt a tranzakció, ezzel párhuzamosan pedig a címeken lévő bitcoinok összege nullára csökken. A tranzakcióra jobb gombbal kattintva, majd a *Details* parancsot választva előhívhatjuk a tranzakció részleteit tartalmazó ablakot.

10. számú ábra



A *Status* bejegyzés mellett láthatjuk, hogy a tranzakciót hány alkalommal erősítették meg *(confirmation)* a bányászok. Elméletileg előfordulhat, hogy a hatósági tranzakció elindítását követően a lefoglalást szenvedő is indít egy tranzakciót ugyanarról a címről, és – ha magasabb jutalékot ad meg – a bányászok az ő tranzakcióját erősítik meg előbb.

Ez csak úgy előzhető meg, ha a lefoglalást szenvedőt felügyelet alatt tartjuk mindaddig, míg a tranzakció legalább egy – de inkább két – megerősítést nem kap (ergo a blokkba foglalást követően már egy újabb blokkot is kibányásztak). Két megerősítést követően már közel lehetetlen egy tranzakciót felülírni a blokkláncban, így a lefoglalást sikeresnek tekinthetjük.

Mivel a tranzakció ekkor már a nyilvános blokklánc része, ezért az ellenőrzést akár bármely erre szolgáló weboldal segítségével is elvégezhetjük. A

példában szereplő tranzakció a https://blockchain.info/ oldalon az előbbiek szerint néz ki.

Ha mindezt végrehajtottuk, akkor már „csak” azt kell megoldanunk, hogy az utalásban érintett címekhez tartozó privát kulcsokat a továbbiakban is biztonságban őrizzük.

A bitcoin tárolása az eljárás során

Bár a lefoglalás lépéseinek bemutatásakor egyben ajánlást adtam arra vonatkozóan is, hogy milyen módon történjen a lefoglalt bitcoin tárolása, azonban ez a módszer csak abban az esetben alkalmazandó, ha nem áll rendelkezésre erre vonatkozóan központi megoldás.

Mindenekelőtt fontos leszögezni, hogy a bitcoint a lefoglalást követően a hatóság nem értékesítheti abból a célból, hogy az eljárás végéig pénzként tárolja azt a letéti számláján (a kapcsolódó konferenciák során gyakran hallok erre vonatkozó „javaslatokat”). Bár ez elsőre talán kézenfekvő megoldásnak tűnhet, azonban több akadálya is van.

Egyrészről a 11/2003. (V. 8.) IM–BM–PM együttes rendelet alapján letéti számlára csak lefoglalt pénzt lehet befizetni – magyar pénzt a hatóság által kezelt, külföldi pénzt pedig a Magyar Államkincstár által vezetett letéti számlára –, a bitcoin pedig jogilag nem tekinthető pénznek.

Másrészről pedig a lefoglalt dolgok előzetes értékesítéséhez szükséges feltételek[34] egyike sem igaz a bitcoinra – a bitcoin ugyanis nem romlandó, nem alkalmatlan huzamos tárolásra, az nem jár jelentős költséggel, illetve az sem jelenthető ki, hogy a hosszú tárolás miatt értéke biztosan csökkenne.[35] Márpedig ezek a törvényben taxatíve felsorolt feltételek, az előzetes értékesítésnek más esetköre nincs.[36]

Érdemes megjegyezni továbbá, hogy ha nem lennének jogi akadályai az előzetes értékesítésének, az akkor sem lenne indokolt. A bitcoin árfolyama ugyanis rendkívül nagy ingadozást mutat (néhány éves története során az értéke több ezerszeresére növekedett, majd újból csökkent), és ha a lefoglalás után az értéke újból növekedne, akkor a számlán lévő forintösszeg már nem

34 Be. 156. § (1) bekezdés

35 Az utolsó pont kapcsán meg kell jegyezni, hogy a bitcoin értéke a tárolás során valóban csökkenhet ugyan, ám éppúgy nőhet is, a törvény pedig csak akkor teszi lehetővé az előzetes értékesítést, ha a csökkenés bizonyosan bekövetkezik a hosszú tárolás miatt.

36 E feltételek az új Be.-ben is változatlanok [új Be. 319. § (3) bekezdés].

fedezné az értékét. Ha valamely okból a lefoglalás megszüntetésére kerülne sor, akkor a bitcoin tulajdonosát érdeksérelem érhetné, amiért akár jóval kisebb pénzösszeget kap vissza, mint amit a bitcoinjai egyébként érnének.

Mivel a bitcoin lefoglalására jellemzően nem a bizonyítás (hiszen arra tökéletesen alkalmas a blokklánc), hanem a vagyonelkobzás későbbi biztosítása érdekében kerül sor, így a hatóság a lefoglalást arra való hivatkozással sem szüntetheti meg, hogy arra a bizonyítás érdekében már nincs szükség. A lefoglalt bitcoin ezért jellemzően az eljárás végéig a hatóság őrzésében kell hogy álljon, amíg az eljárást valamilyen okból meg nem szüntetik, vagy ítélettel a vagyonelkobzást a bíróság meg nem állapítja.[37]

Fel kell készülni tehát arra, hogy a bitcoin őrzéséről hosszú ideig kell a hatóságnak gondoskodnia. És bár ez csak a privát kulcsok megőrzését jelenti, azonban amennyire mindez egyszerűnek hangzik, egyúttal éppoly bonyolult is.

A privát kulcs megismerése esetén ugyanis bárki, a lebukás rendkívül kis kockázatával képes lehet megszerezni a bitcoint, ami sajnos súlyos veszélyt jelent. Bár szeretnénk azt hinni, hogy a hatóság tagjai feddhetetlenek, azonban a büntetőeljárás során lefoglalt dolgok jellemzően sok kézen mennek keresztül a nyomozás során, és egyszerűen csak megbízni e kezek feddhetetlenségében túlzott könnyelműség lenne.[38]

Kézenfekvőnek látszik, hogy a privát kulcsok elkészítését és őrzését bízzuk csupán egyetlen személyre, hiszen ilyenkor egyértelmű, hogy a bitcoin eltűnése esetén ki a felelős. Ilyenkor azonban számolnunk kell azzal a kockázattal, hogy ha ezzel a személlyel később történik valami, vagy egyszerűen csak elveszti a kulcsokat, és rajta kívül senki nem fér hozzájuk, akkor a hatóság maga veszíti el a rendelkezés lehetőségét. Két személy esetén viszont már sosem lehetünk biztosak benne, hogy melyikükben keressük a felelőst.

Látható tehát, hogy meg kell találni a kényes egyensúlyt a privát kulcsok illetéktelen kezekbe kerülésének, illetve azok elvesztésének kockázata között olyan módon, hogy számottevően egyik tényező miatt se kelljen aggódnunk.

37 Érdekes kérdés, hogy az új Be.-ben megjelenő megváltás intézménye (318. §) miként jelentkezik majd a gyakorlatban a bitcoinlefoglalások során. Egyes nyugati országokban régóta gyakorlat, hogy a bitcoin lefoglalását követően a lefoglalást szenvedőt írásban nyilatkoztatják, hogy mi a kívánsága: a hatóság adja el rögtön a bitcoint az adott árfolyamon, vagy pedig bitcoinként őrizze azt továbbra is az eljárás végéig. Hasonló módszerre akár a megváltás intézménye is lehetőséget adhat, azonban itt a tulajdonosnak kell visszavásárolnia a lefoglalt bitcoint a hatóságtól, és ennek engedélyezése is ez utóbbitól függ.

38 Találhatunk példát arra vonatkozóan, amikor éppen a csábításnak ellenállni nem tudó nyomozó tulajdonította el az eljárás során lefoglalt bitcoint. FBI Agent Admits to Stealing Silk Road Bitcoins Seized by U.S. Marshals. https://news.bitcoin.com/rogue-silk-road-agent-admits-to-stealing-bitcoins-seized-by-u-s-marshals/

Az általam vázolt megoldás ideig-óráig használható ugyan, hosszú távon azonban nyilvánvalóan nem fenntartható. Egyrészről mindenképpen bele kell helyeznünk a teljes bizalmunkat abba a személybe, aki a privát kulcsokat létrehozza, hiszen semmilyen módon nem ellenőrizhetjük, hogy azokat a folyamat során nem másolja le. Másrészről a privát kulcsok adathordozón való tárolása a bűnjelkamrában nem olyan megoldás, amit a bitcoin megszerzése érdekében elszánt személy ne tudna feltétlenül kijátszani, főként hogy valószínűsíthetően az esetleg létrehozott jelszót tartalmazó papír is pontosan ugyanebbe a bűnjelkamrába kerülne. Harmadrészről irreális azt feltételezni, hogy a rendőrségen belül ma a kapitányságok nagy részében hajlandók lennének elkülöníteni egy külön számítógépet csak azért, hogy azon bitcoincímeket hozzanak létre, és semmi másra ne használják (márpedig másképpen nem biztosítható, hogy a címek biztosan ne kompromittálódhassanak a készítés során). Negyedrészről pedig számításba kell venni azt is, hogy a nyomozók nagy részének nincsenek mélyebb ismeretei arról, hogy mi is pontosan a bitcoin, és milyen hibalehetőségekre kell különösen odafigyelni egy privát kulcs létrehozása és tárolása során, így – akár rendelkezésére áll egy útmutató, akár nem – a véletlen hibázás lehetőségével is számolni kell.

Mindezen tényezők egyesével is jókora kockázatot hordoznak magukban, így összességükben pedig mindenképpen azt feltételezik, hogy a biztonságos tárolás fenntartása hosszú távon csak központi intézkedés útján lehetséges.

A blokklánc jellegéből adódóan azonban semmi akadálya nincs annak, hogy a rendőrségen központi szinten, a szükséges szakértelemmel és biztonsággal elkészítsenek egy megfelelően őrzött címet, amit ezt követően minden alsóbb szerv egyformán használhat az összes lefoglalás során. Ezzel egyrészről levesszük a hibázás kockázatának terhét az alsóbb szintű nyomozó szervek dolgozóiról, másrészről nem terheljük őket a hosszú megőrzés jelentette felelősséggel sem, harmadrészről pedig nem is tágítjuk ki azon személyek körét, akikben kénytelenek vagyunk vakon megbízni.

Nem kell attól tartani, hogy az így létrehozott címen a különböző helyekről érkező lefoglalt bitcoinok „összekeverednek”, hiszen a blokklánc elvégzi helyettünk a „jegyzőkönyvezést”, és pontosan nyilvántartja, hogy mikor, honnan és mekkora összeg érkezett a címre.

Felvetődik azonban a kérdés, hogy kit bízzunk meg az így létrehozott címhez tartozó privát kulcs őrzésével. Mint láttuk, egy személy megbízása is kockázatos (a kulcs elvesztésének veszélye miatt), és több személy sem jelent megnyugtató megoldást (a felelősség megállapításának nehezülése miatt).

Szerencsére azonban a bitcoinprotokoll lehetővé teszi olyan címek létrehozását is, amelyek fölötti rendelkezéshez egyszerre több privát kulcs együttes megléte szükséges (ezeket hívják *multisignature* – több aláírást igénylő – címeknek vagy tárcáknak).

E *multisignature* címek valódi előnye azonban abban rejlik, hogy az aláírások szükségességének bármilyen kombinációja beállítható: minden további nélkül meghatározhatjuk például, hogy egy adott címhez három privát kulcs tartozzon, és az utalás kezdeményezéséhez ebből a háromból bármely kettő együttes meglétére legyen csupán szükség.[39]

Mindez tökéletes megoldást nyújt az előbb említett problémára, hiszen ennek a módszernek az alkalmazásával megbízhatunk két különböző személyt a rendőrség szervezetén belül egy-egy privát kulcs őrzésével, és a kiutalásokat egyikük sem fogja tudni a másik hozzájárulása nélkül kezdeményezni. Ugyanakkor attól sem kell tartanunk, hogy valamelyikük a privát kulcsot elveszíti és ezzel a bitcoinhoz való hozzáférést ellehetetleníti, ugyanis ilyen esetben még mindig rendelkezésre áll a harmadik – addig akár letétben tartott – privát kulcs is.

Mivel a közös címről történő kiutalásokra csak az eljárások legvégén kerül sor, így várhatóan csak viszonylag ritkán lesz szükség utalások végrehajtására. Ebből kifolyólag elképzelhető megoldás lehet akár az is, hogy a privát kulcsok egyikét a rendőrség, míg a másikat az ügyészség őrizze, a minimálisra csökkentve ezzel a lehetséges összejátszás veszélyét.

Álláspontom szerint – bár a bitcoinlefoglalások jelenleg még nem részei a nyomozó hatóságok mindennapi munkájának – az új büntetőeljárási törvény hatálybalépésével és a bitcoinnal kapcsolatos bűncselekmények számának folyamatos növekedésével a jövőben igenis számolni kell az effajta esetek megjelenésével. Mindehhez pedig elengedhetetlen egy olyan biztonságos rendszer létrehozása, amely lehetővé teszi a nyomozó szervek mindegyike számára a megőrzés egyszerű, átlátható és biztonságos módon történő végrehajtását.

39 Pedro Franco: Understanding Bitcoin: Cryptography, engineering, and economic. Wiley, 2014, pp. 136–137.