Eszteri Dániel
PhD-hallgató

Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze?

1. Bevezetés[1]

Pénzhez sokféleképpen juthatunk. Megkereshetjük munkával, kaphatjuk ajándékba, találhatjuk az utcán, hamisíthatunk magunknak vagy ellophatjuk másoktól. Ezek viszonylag hagyományos módszereknek számítanak a világban, akár törvényesek, akár büntetendőek a jog szerint. Mi a helyzet azonban akkor, ha kitalálunk egy újfajta pénzt?

Az interneten létező Bitcoin nevű virtuális pénz – amelyet magyarul Bitérmének fordíthatunk –, egy újfajta független fizetőeszköz, amely nevéhez hűen teljes mértékben bitekből áll, azonban fizikai megtestesülésével, érmeként vagy bankjegyként sehol sem találkozhatunk vele. Nincs mögötte fedezet áruban, aranyban vagy bármilyen más nyersanyagban, csupán az a harmincegyezer sornyi forráskódból álló szoftver, amivel hozzáférhetünk a teljesen virtuális fizetőeszközhöz.[2]

2008 novemberében kezdődött el az egyedülálló virtuális valuta karrierje, amikor egy magát Satoshi *Nakamotónak* nevező ismeretlen személy megjelentette az interneten híres tanulmányát,[3] amelyben egy kizárólag a virtuális térben létező pénz megalkotásának folyamatát mutatja be.

A cikk írójáról senki sem hallott azelőtt, még a kriptográfiában jártas nagy öregek is csak hallgattak, amikor először meglátták leírva ezt a nevet. Nakamoto nem volt egyéb egy rejtélyes, arcnélküli hacker online profiljánál, amely mögött állítása szerint egy japánban élő programozót kell érteni. Az e-mail címet, amelyről a tanulmányt közzétették egy németországi anonim domain regisztrátornál vették nyilvántartásba, a világhálón pedig semmilyen egyéb lényeges információ nem lelhető fel róla. Mégis, ez a rejtélyes személy – aki azóta egyszer, s mindenkorra felszívódott az internet mélységes mély bugyraiban – egy olyan kérdésre adta meg a választ, amely a világháló létezése óra kétségbe ejti a kriptográfiával és digitális fizetőeszközökkel foglalkozó szakembereket.[4] Az érméket kezelő program nyilvánosságra hozatala és az első Bitcoinok forgalmazása 2009 januárjában indult meg, a Nakamoto tanulmánya alapján létrehozott online hálózaton keresztül, amely logikailag a decentralizált peer-to-peer rendszerek (mint pl. a fájlok megosztására használható bittorrent technológia) mintáját követi.

A jelenség persze rengeteg kérdést felvet már első ránézésre is. Mi is az a Bitcoin? Mennyi az értéke egy Bitcoinnak? Hogyan fizethetünk vele? Mire használhatjuk, és miket vehetünk rajta? Biztonságos e egyáltalán a technológia, hogy ha nincs mögötte semmilyen állami garancia vagy szervezet? Hogyan juthatunk hozzá és állíthatjuk elő? Miként működik a rendszer, biztonságos-e és milyen jogi keretei vannak? Felhasználható-e illegális tevékenységekhez az újfajta fizetőeszköz? Tanulmányomban többek között ezekre a fő kérdésekre keresem a választ.

2. A Bitcoin elődeiről

A pénz történetének legutóbbi fejezeteit a virtualizáció határozta meg. A papírpénz alternatívájaként megjelent a tényleges pénzmozgást a kibocsátó bankokra redukáló hitelkártya, aztán pedig az értéket adatsorokban tároló, a kibocsátó bank digitális aláírásával hitelesített, a fizetőeszközök közül a legkisebb működési költséggel járó digitális pénz. Utóbbinak a hagyományos funkciók[5] mellett több új kritériumnak is meg kell felelnie: biztonság, anonimitás, elfogadottság, különböző címletek, offline működés, a működtető rendszer skálázhatósága és hardver-függőség.[6]

A Bitcoin megjelenését megelőzően többen is foglalkoztak az anonim, független és decentralizált digitális fizetőeszközök elméletének kidolgozásával. A problémát a 90-es években először Timothy *May* és az eszméit az interneten népszerűsítő cyberpunk-hívők[7] vázolták fel, akik a privátszféra megvédését tekintették az elkövetkező évtizedek legfontosabb problémájának. A csoport tagjai a May által alapított *„Cyberpunks electronic mailing list"* nevű internetes levelezőlistán osztották meg véleményüket egymással. May elméleteit *„Crypto Anarchy, Cyberstates, and Pirate Utopias"* című 2001-ben megjelent, Peter Ludlow által szerkesztett könyv foglalja össze.[8]

Szintén a 90-es évek elején kísérletezett egy független online fizetőeszköz, az *Ecash* bevezetésével David *Chaum*. Az ötlete azonban megbukott, mivel a fizetőeszköz hiánytalan működése mindenképpen feltételezte a kormány és bankkártya kibocsátó szervezetek létét.[9]

A fentieket továbbfejlesztve alkotta meg Wei *Dai* 1998-ban a *B-money* ötletét. Gondolatmenetében felvázolta, hogy a virtuális fizetőeszköznek munkabizonyítékokra kell épülnie, másrészt a rendszerben a jegyzőknek algoritmikus módon kell megegyezniük a készlet bővítéséről.[10]

Nick *Szabó* szintén 1998-ban dolgozta ki a *bit-arany*, az interneten létrehozható hamisíthatatlan, ott biztonságosan tárolható, átutalható és könnyen ellenőrizhető – az aranyhoz hasonlóan funkcionáló – bitek elméletét, amely széleskörű nyilvánosságra csak 2005-ben került.[11] Az elmélet alapja, hogy a feleknek a lehető legkevesebb mértékben kelljen csak bármiféle bizalmas harmadik félre hagyatkoznunk. A résztvevők számítógépes kapacitásuk egy részét az elosztott rendszer által kijelölt kriptográfiai egyenletek megoldására szentelik.[12]

Ezek az elméletek már a Bitcoin megszületését vetítették előre, hiszen annak rendszere is tartalmaz olyan elemeket, amelyek a fenti teóriákból köszönnek vissza. A következő fejezetekben, az immár a gyakorlatban is megvalósult Bitcoin rendszer működésének felvázolása következik.

3. A Bitcoin, mint virtuális fizetőeszköz alapvető tulajdonságai

A Bitcoin (általános rövidítése: BTC) nem kézzelfogható, fizikailag létező fizetőeszköz, hanem virtuális pénz: egy összeg, amely társítva van egy virtuális pénztárcával.[13] Hogyan is juthatunk hozzá egy ilyen pénztárcához? Először is le kell töltenünk egy ingyenes szoftvert az internetről, melyet szintén Bitcoinnak hívnak. A programot a virtuális fizetőeszköz hivatalos honlapján találhatjuk meg.[14]

Ez a program egyfajta virtuális pénztárcaként funkcionál a számítógépünkön, mely digitális pénzünket tárolja. A pénztárcánk nem más, mint egy fájl a számítógépen, amit „*wallet.dat*" néven találhatunk meg.[15] Ezen tulajdonsága miatt a szó legszorosabb értelmében akár el is lehet lopni tőlünk, ha valaki illetéktelen behatol a rendszerbe. Ennek megakadályozása érdekében érdemes biztonsági másolatokat készíteni a fájlokról, de léteznek olyan internetes szolgáltatások, ahová regisztrálva feltölthetjük a tárcánkat és ahhoz csak megadott jelszavunkkal férhetünk hozzá.[16] A program nyílt forráskódú, mely minden jelentősebb operációs rendszerre lefordított változatban elérhető, folyamatosan fejlesztik, és a Bitcoinok küldéséhez és fogadásához szükséges minden funkciót tartalmaz.[17]

Miután számítógépünkre sikeresen telepítettük a fenti szoftvert, nincs is más hátra, mint hogy elindítsuk, és akár kezdődhet is a virtuális kereskedés. Arról, hogy mégis hogyan juthatunk Bitcoinokhoz a későbbiekben lesz szó.

A virtuális pénztárcaként funkcionáló program azonban csak a jéghegy csúcsa, hiszen adja magát a kérdés, hogy mégis hogyan lehet egymásnak pénzt küldeni vele. Nos, erre szolgálnak az úgy nevezett Bitcoin-címek, amiket szintén ezzel a szoftverrel készíthetünk magunknak. Minden egyes felhasználó rendelkezik legalább egy ilyen Bitcoin-címmel, amely logikailag egy e-mail címhez hasonlatos. Különbség a kettő között, hogy ezzel nem szöveges üzeneteket és fájlokat, hanem virtuális pénzt küldhetünk és fogadhatunk.

A Bitcoin-címünket a virtuális pénztárca-szoftver kérésünkre automatikusan generálja. A program elméletileg minden egyes tranzakciónkhoz külön címet készít, növelve ezzel az anonimitást, és a rendszer biztonságát. Persze ha megadjuk valamilyen nyilvános fórumon egyik címünket, akkor ezt több átutalásra is fel fogja használni a program, viszont ez csökkenti az anonimitást. Ez akkor fordulhat elő, ha például adományok reményében publikáljuk valahol egyik címünket. Az egyszer már létrehozott címeinket nem törölhetjük ki, hanem azokat a digitális pénztárcánkban bármikor visszakereshetjük és megnézhetjük, hogy adott címről mennyi pénzt kaptunk, illetve mennyit utaltunk át másoknak.

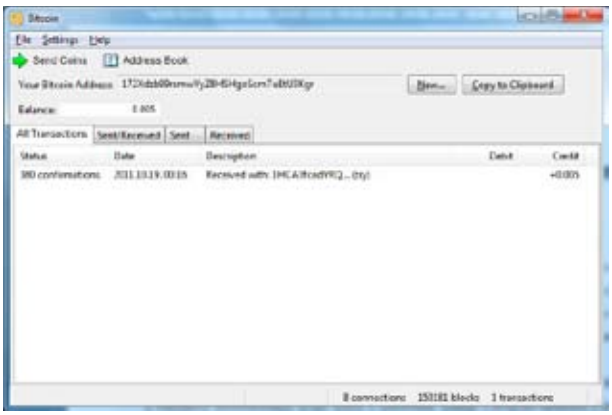
Mindegyik Bitcoin-cím két részből. Az egyik része az úgy nevezett „*nyilvános kulcs*", a másik pedig a „*privát kulcs*". A nyilvános kulcsunkat mi magunk is láthatjuk, amikor belépünk a programba a „*Your Bitcoin Address*" sorban, a címhez tartozó privát kulcs azonban rejtve marad. Címünk nyilvános kulcsának olvasható formája általában 33 karakterből áll, és mindig egyessel kezdődik, például: *1HCA3fcadYRQk5Sm3WGD2CPxsZqhdRXTY9*. A Bitcoin-címünkhöz tartozó ilyen nyilvános kulcsot kell megadnunk másoknak, amikor a Bitcoin-hálózaton keresztül pénzt szeretnénk küldeni egymásnak.[18]

A tranzakciók hitelesítéséhez azonban a program nem a nyilvános-, hanem a „*privát kulcsot*" használja, amely ugyanúgy az általunk generált címhez tartozik, azonban az mások számára nem látható. Ez a privát kulcs egyfajta elektronikus aláírásként funkcionál. A pénzügyi tranzakcióink aláírásához a program ezt a privát kulcsot használja, növelve ezzel a biztonságot. A nyilvános kulcsokat és hozzájuk tartozó privát kulcspárokat a már említett wallet.dat nevű fájlban tárolja a program a számítógépünk merevlemezén. A privát kulcsokat csak itt tudjuk megnézni, és ha csak nem akarjuk, hogy mások ellopják az érméinket akkor ne is adjuk meg őket senkinek. Ellentétben a publikus kulcs megadása minden esetben szükséges a tranzakcióhoz.[19] Hogyan is történnek a tranzakciók, és mi a funkciójuk a címekhez rendelt nyilvános- és privát kulcsoknak?

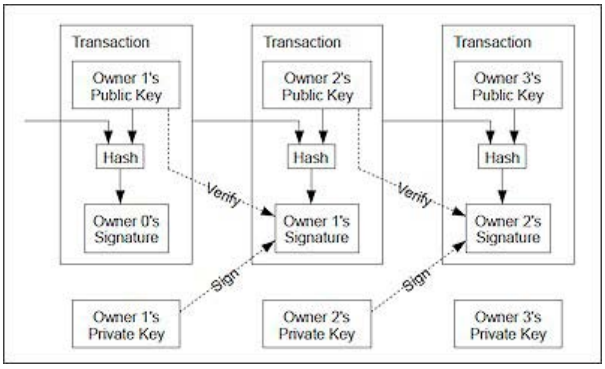
A Bitcoin hálózat a rajta keresztül létrejövő tranzakciókat az egész hálózaton szétküldi, így azok teljesen nyilvánosak. Szemben a hagyományos pénzügyi intézetekkel, amelyek az ügyfelek magánszféráját a tranzakciókra vonatkozó információk visszatartá-

sával védik, ezt a Bitcoin rendszerében az biztosítja, hogy a címek tulajdonosaira vonatkozó információk egyáltalán nem ismertek.[20] Ha például létrehozok a Bitcoin szoftverrel egy új címet, akkor a program semmilyen információt nem kér tőlem a személyes adataimat illetően. Nem kell magunkat regisztrálni a hálózatra, egyszerűen csak el kell indítanunk a programot, amely aztán az általa generált címekre kapja másoktól a digitális pénzt és elmenti azt a számítógépünkön a virtuális pénztárcánkba. A rendszer működésére nézzünk egy egyszerű példát.

Tegyük fel, hogy Aliz szeretne küldeni Bencének 10 Bitcoint. Bence ezért megadja Aliznak a virtuális pénztárcájához tartozó Bitcoin-címét – vagyis szűkebb értelemben véve az ehhez a címhez tartozó nyilvános kulcsot. Ez az a 33 karakterből álló kód, amiről fentebb is szó volt és a szoftver kijelzi nekünk. Ha Bence több címet is generált a pénztárcájához, bármelyiket megadhatja, vagy akár készíthet egy újat is csak ehhez az utaláshoz. A pénz végül mindenképpen Bence pénztárcájában fog landolni a számítógépén, függetlenül attól, hogy azt melyik címen kapta Aliztól. Miután Aliz megtudta, hogy mi Bence címe, egyszerűen rákattint a Bitcoin szoftverben a „*Send coins*" („érmék küldése") gombra. A felugró ablakban meg kell adnia Bence címet és az összeget, amit át szeretne neki utalni. Aliz ezután a „*Send*" („küldés") gombra kattintva jóváhagyja a tranzakciót és ezzel véget is ért az utalás azon része, amelyet emberi kéz végez.



A folyamat azonban itt nem ér véget. A szoftver ugyanis Aliz privát-kulcsát fogja használni a tranzakció hitelesítéséhez, kvázi aláírja a szerződést. Ezután a program szétküldi a hálózaton a tranzakciót, amelyet bárki láthat. A nyilvánosság számára azonban csak annyi lesz látható, hogy a „*172Xdzb99rsmwVyZ8HSHgoScmTuEtU3Kgr*" nyilvános kulccsal rendelkező címről a „*12HnGCwvS4ES1tRC3JXeEYHuFLs9mzMjF7*" nyilvános kulcsú címre 10 Bitcoin érkezett. Mivel az elektronikus aláírásként funkcionáló privát-kulcsokat nem látja senki, és mivel akár minden egyes érme elküldéséhez külön-külön címet (tehát nyilvános- és privát kulcs párt) használhatunk a rendszer teljesen anonim módon használható. Később, ha Bence át akarja utalni ezt az összeget Csabának, ugyanezt kell tennie. Csaba megadja Bencének a nyilvános kulcsát, majd ezt a kulcsot használva Bence beírja, hogy mennyi pénzt szeretne küldeni neki. A program ezután ugyanúgy aláírja a tranzakciót, de immár Bence *privát*-kulcsával. Az utálás a hálózaton keresztül ugyanolyan módon mindenki számára látható válik, mint az előző esetben.



Ha Diána el akarja lopni Bence Bitcoinjait, nem tudja ezt úgy megtenni, hogy egyszerűen átírja a saját *nyilvános*-kulcsát Bencéére, mivel még Aliz írta alá a tranzakciós szerződést az ő *privát*-kulcsával, mely arról tanúskodik, hogy a kérdéses összeg Bencét illeti. Az átutalásokhoz pedig mindkét kulcs egyszerre szükséges. Mivel Diána nem tudhatja Aliz *privát* kulcsát, nem hajthatja vége még egyszer az utalást, így a lopás technikailag kizárt.[21] A tranzakciókat az alábbi ábra szemlélteti.[22]

4. A decentralizált hálózat

A fentiekből kiderült, hogy a Bitcoin meglehetősen biztonságosan használható a hálózaton keresztül, hiszen a címekkel való trükközéssel történő lopás esélye gyakorlatilag kizárt. A rendszert okosan kihasználók tökéletes anonimitásba burkolódzhatnak, így a személyes adatok védelme is megoldott. Ez azonban nem garancia arra, hogy esetleg ugyanazt az összeget kétszer is el tudnánk utalni, ami a pénzhamisítás virtuális formája. A kétszeres költés lehetőségét a rendszer az alábbiak szerint zárja ki.

Egy központosított rendszerben a csalást úgy előzik meg, hogy az összes tranzakció átfolyik egy központi adatbázison, mely tárolja azok adatait és így kiszűri az olyan későbbi utalásokat, amelyek mögött nincs fedezet. Ha az egyik felhasználó még egyszer el akar költeni egy olyan összeget, ami nem áll valójában a rendelkezésre, azt nem teheti meg, mivel a rendszer vissza fogja dobni a kérését.

A Bitcoin rendszer ezzel szemben épphogy decentralizált, melyben nincs központi adatbázis, szerver vagy bármilyen egyéb hatóság, ami ezt az ellenőrzést végzi. Sok eddigi decentralizált virtuális pénz létrehozására törekvő kísérlet bukott meg azon, hogy a dupla-költés lehetőségét csak úgy tudták kizárni, ha felállítottak egy központi hatóságot, ami ezt ellenőrizte. A virtuális pénzek így hasonlóvá váltak a valódi pénzekhez, hiszen a bankok is ilyen ellenőrzést végeznek.

Szükséges volt tehát a Bitcoin-rendszer számára valamilyen más megoldást találni, ami megakadályozza, hogy az érmetulajdonos már előre alá tudjon írni kulcsával tranzakciós szerződést, és ezzel esetleg kétszer eladni ugyanazt az érmét. Ennek megoldására, először azt a szabályt kell felállítani, hogy csak az időben legelső tranzakció számít és az összes többi utána következő érvénytelen, ami ugyanarra az érmére szól. Ez viszonylag egyszerű szabály, melynek betartását a központosított rendszerben egy erre kitalált szerv, például egy bank végezte. A Bitcoin decentralizált rendszerében ez csak úgy oldható meg, ha minden egyes tranzakció nyilvános, és bárki számára megtekinthető.[23] Ez azonban nem minden, hiszen kinek lenne arra ideje, hogy ezeket ellenőrizgesse? A rendszer ezt a következőképpen oldja meg. Először is minden tranzakción végigfuttat egy hash algoritmust. A hash algoritmusok egyirányú kódolási módszerek, melyet a számítógépes adatok titkosításánál is használnak. Az algoritmus a számítógépes adatokat konvertálja számokká, melyet hash értéknek hívunk. Ha ez a szám elég hosszú, akkor teljesen azonosíthatóvá tesz valamilyen egyedi adatot. A hash-szám egyértelműen utal a titkosított adatra, azonban belőle nem állítható elő visszafejtéssel az adat, amit titkosított. Viszont a számot használva ellenőrizhetjük, hogy valóban azzal az adattal van e dolgunk, amire szükségünk van.[24]

Minden Bitcoin átutalás során a küldő fél a privát kulcsával, tehát digitális aláírásával látja el az előző tranzakció hash értékéből és a következő tulajdonos, tehát a fogadó fél publikus kulcsából álló csomagot. Ezzel igazolja, hogy a csomagot és a benne található Bitcoin-összeget tényleg a fogadó félnek szánta.[25] A hash, a cím és az aláírás naplózódik az interneten, az úgy nevezett *blokkok*-ban, amiket a *blockexplorer.com* című honlapon meg is nézhetünk. Ezek a blokkok adathalmazok, melyekben megtalálható a világon elérhető minden Bitcoinonnal végzett művelet naplózása. A szokásos banki modellektől eltérően nem a tranzakciók titkosak és a számlatulajdonosok ismertek, hanem éppen fordítva. A Bitcoin kliens a beüzemelése után minden egyes felhasználónak letölti az összes blokkot a számítógépe merevlemezére (jelenleg kb. 190 ezret, ami hozzávetőlegesen 400 MB), később pedig hozzá mindig a legújabbakat. Ilyen redundanciával a világ legbiztonságosabb banki adatbázisa sem rendelkezik.[26] Az összes tranzakció teljes adatbázisa megtalálható minden egyes ember számítógépén, aki Bitcoint használ és az a nyílt hálózaton keresztül folyamatosan frissül. Ahhoz, hogy egy utalás teljesülhessen legalább hat másik a hálózatra kapcsolódott számítógépnek kell igazolnia a tranzakciót, így a csalás gyakorlatilag kizárt.[27]

Egy idő után ez tarthatatlan lesz, mivel a tranzakciók számának növekedésével a blokkok mérete is nőni fog, ezért később lehetőség lesz arra, hogy a tranzakciónaplónak csak a releváns részeit töltse le a program.[28] Ez azonban még a jövő zenéje. A blokkok szerepéről később még több szó fog esni.

A tranzakciók címzettje csak úgy tudja igazolni magát (vagyis további tranzakciókra felhasználni a pénzét), ha rendelkezik a csomagban lévő nyilvános kulcsához tartozó privát kulccsal is. A nyilvános és privát kulcspárok a virtuális pénztárcánkban tárolódnak a számítógépünkön a *wallet.dat* fájlban, éppen ezért a Bitcoin világában ezek a fájlok számítanak a legféltettebb kincseknek.[29] Érdemes róla sűrűn biztonsági másolatot készíteni és nem csak egy számítógépen tartani. A virtuális pénztárcánkban lévő kulcspárokat a szoftver összeveti a blokkokban tárolt tranzakciós információkkal és ez alapján számolja ki, hogy mennyi Bitcoin van a zsebünkben. Ezek alapján nem meglepő, ha a Bitcoin kitalálója, Nakamoto szerint *egy virtuális érme nem más, mint digitális aláírások láncolata*.[30] Talán legjobban a névre szóló értékpapírokhoz tudjuk ezek alapján hasonlítani a Bitérmét, hiszen az ilyen értékpapírokhoz tartozó forgatmányban is ugyanígy vannak feljegyezve, hogy azokat ki, mikor és kire ruházta át.

5. „Bitcoin bányászat"

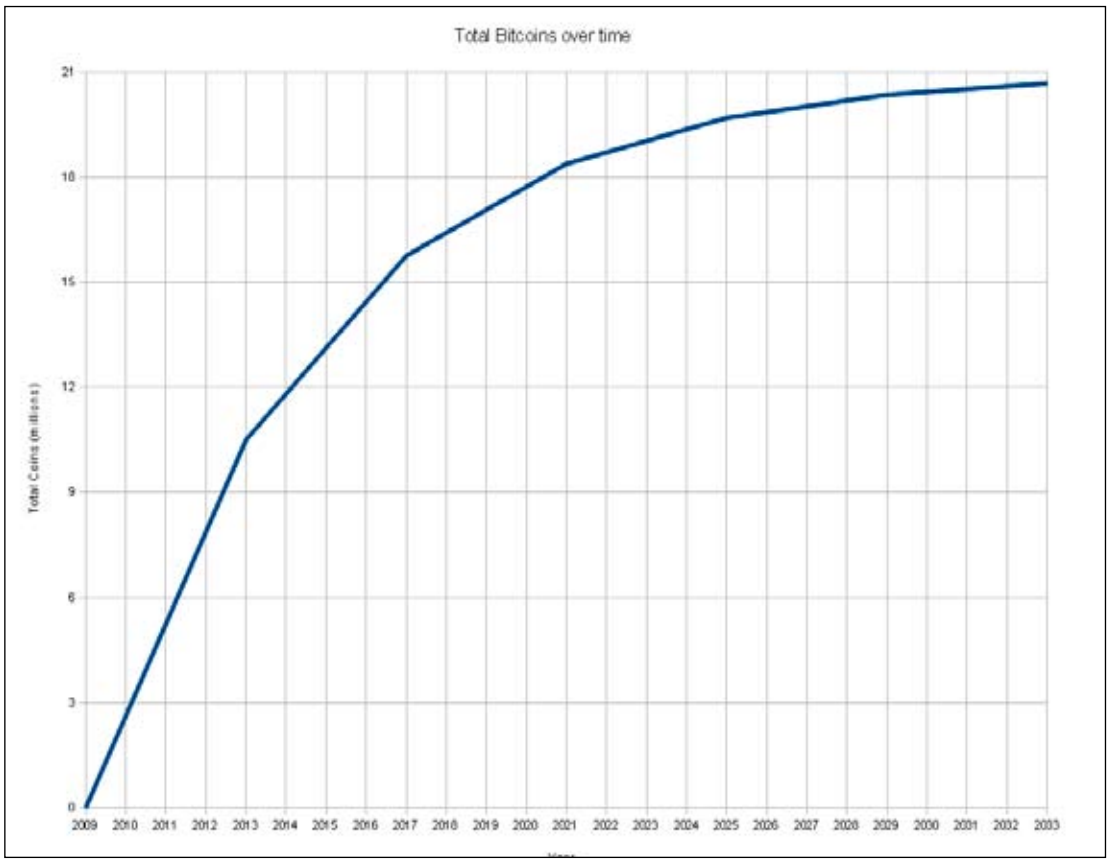
Mivel a Bitcoinoknak nincs központi kibocsátója, felmerül a kérdés, hogy vajon mégis hogyan szerezhetünk belőlük magunknak? Nos, egyrészt vehetjük őket más Bitcoin tulajdonosoktól, vagy nekifoghatunk mi magunk is a termelésének. Mit is kell érteni termelés alatt?

Az új érmék a Bitcoin hálózat csomópontjain generálódnak, amikor a rendszer megoldást talál egy bizonyos matematikai problémára.[31] Ahhoz, hogy mi is hozzájárulhassunk a Bitcoinok ilyen úton történő előállításához le kell töltenünk egy szoftvert, amely az után a számítógépünk processzorának, vagy videokártyájának erőforrásait használja az ilyen matematikai problémák megoldásához eszközül. Ezeket a programokat „*bányász-szoftvernek*" („mining-software") nevezzük, amely a fentebb említett virtuális

pénztárca szoftvertől teljesen független program.[32] Ha sikerült megoldatni a számítógépünkkel a Bitcoin-hálózaton egy matematikai algoritmust, létrejön egy úgy nevezett blokk, amelyekben a bitérmék tárolódnak és ezen kívül tartalmazza a velük végzett tranzakciós adatokat is, mint ahogy arról már fentebb szó volt.[33] Egy ilyen blokk megtalálása jelenleg 50 Bitcoint ér, mely 10 perc után (ennyi a rendszer átfutási ideje) virtuális pénztárcánkban landol és akár el is költhetjük vagy átválthatjuk. A blokkok megoldását lehet egyedül is végezni („solo-mining"), vagy csatlakozni egy úgynevezett „*bányász-társuláshoz*" („mining-pool"), amire az interneten keresztül több számítógép is csatlakozik és immár együttes erővel tudjuk dolgoztatni gépeinket érmék generálásán. Az algoritmusok megoldásának nehézsége attól függ, hogy éppen mekkora számítási kapacitással dolgoztatják a Bitcoin bányászok számítógépeiket a hálózaton. Ha sok számítógép csatlakozik, nehezebb megoldani a problémát, ha kevesebb, akkor valamivel könnyebb lesz a munka.

A Bitcoinok azonban nem hozhatók létre végtelen mennyiségben, hiszen ez azt jelentené, hogy ameddig számítógépek, internet és legfőképpen elektromos energia van a Földön, addig végtelen számú virtuális pénz állítható elő, ami rögtön értéktelenné is tenné azt. Ezt a problémát a rendszer úgy oldja meg, hogy előre meg van határozva maximum mennyi érme hozható létre a hálózaton. Ezen felül a blokktalálatoknál a jutalmul kapott érmék száma a blokkok aktuális számától is függ. Egy blokk 50 Bitcoint ér az első 210.000 blokktalálat esetében. A tanulmány írásának idejében (2012 nyara) itt tartunk, tehát ha egy bányász számítógépe megoldást talál egy matematikai problémára és létrejön egy blokk, akkor cserébe 50 Bitcoin üti a markát, illetve egy több személyes bányász-társulat esetén ennyi érme lesz felosztva a tagok között. A rendszer szerint ezután 25 Bitcoint fog érni egy megoldás a következő 210.000 blokk esetében, majd később 12,5 érmét, 6,25-öt és így tovább. Ez azt jelenti, hogy a Bitcoin hálózat első négy évében 10.500.000,- virtuális érme lesz létrehozva (210.000 megtalált blokk szorozva 50 Bitcoinnal).

Ez az összeg megfeleződik minden negyedik évben, így a második négy év során már csak 5.250.000,- kerül megtalálásra (210.000 megtalált blokk szorozva 25 Bitcoinnal). A harmadik négy év során 2.625.000,- és így tovább. Láthatjuk, ahogy az idő telik, úgy termelődik egyre kevesebb érme, és annál több időbe is kerül majd „kibányászni" őket. A virtuális érmék teljes száma idővel a 21.000.000,- Bitcoinhoz fog közelíteni. Az utolsó blokk, amely érmét fog létrehozni, a 6.929.999-ik lesz, amely körülbelül a 2140. évben fog generálódni. Ezután az összes forgalomban lévő érme száma statikus marad, és összesen 20.999.999,- lesz a számuk a világon.[34] A folyamatot az alábbi ábra szemlélteti.[35]



6. Mennyit ér egy Bitcoin?

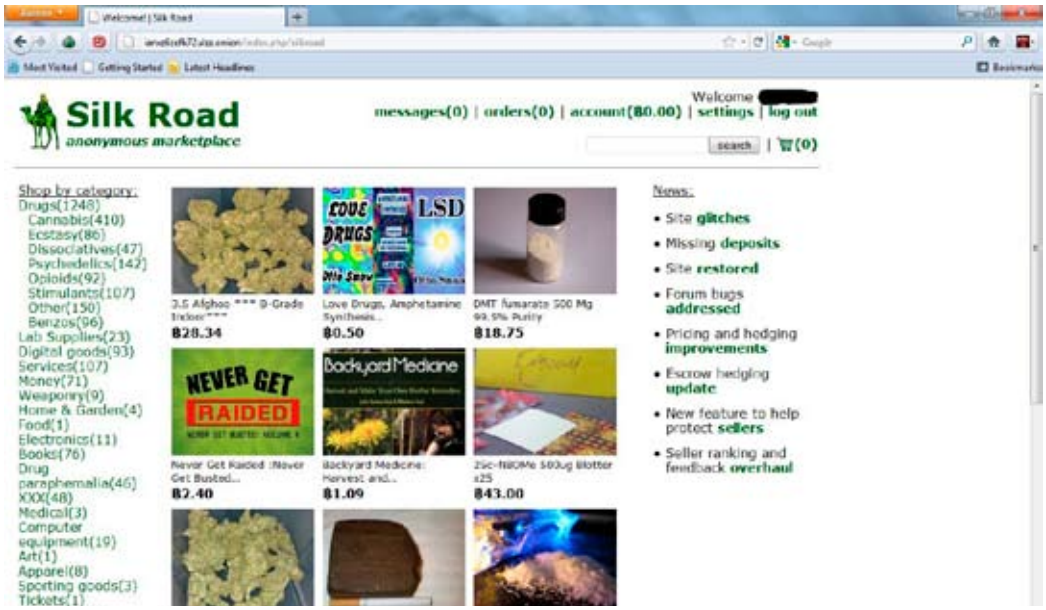
A pénzünket, legyen szó amerikai dollárról, euróról, vagy akár magyar forintról néhány erre specializálódott devizatőzsde honlapon tudjuk Bitcoinra váltani és vissza. Fizetésnél leginkább néhány online szolgáltató fogadja el, illetve felhasználható közérdekű felajánlásokra egyes szervezetnél. Mivel a tranzakciók nem a bankokon, vagy egyéb központi hatóságon keresztül zajlanak, hanem peer-to-peer hálózatokon közvetlenül a felhasználók között – hasonlóan a torrent rendszerhez – ezért a Bitcoin teljesen digitális, decentralizált és anonim fizetési eszköz, mely mögött nem áll semmilyen konkrét jogalany.[36]

Azokból a különböző weblapokból, amelyek a virtuális pénz átváltására vállalkoznak egyre több található az Interneten. A legnépszerűbb USA dollár – Bitcoin váltó a *mtgox.com* címen érhető el, a legnagyobb nyilvános váltók árfolyamairól pedig legegyszerűbben a *bitcoinwatch.com*-on tájékozhatunk.

Arra a kérdésre, hogy mégis mennyit ér egy virtuális érme nehéz konkrét választ adni a folyamatos, és olykor igen drasztikus árfolyam ingadozások miatt. Megalkotásakor 2009-ben egy darab érme alig ért többet pár centnél. Ekkor még könnyű volt Bitcoinokhoz jutni: akár egy középkategóriás otthoni számítógéppel is tudtunk magunknak bányászni több száz érmét. Mivel kevesen csatlakoztak a hálózathoz, így az algoritmusok megoldási nehézsége is nagyon könnyű volt. Miután azonban az emberek elkezdték maguknak felfedezni az új fizetőeszközt és a hálózatban rejlő lehetőségeket, egyre többen kezdtek el bányászni, nőtt a kereslet az új pénz iránt, az árfolyam pedig emelkedésnek indult. 2010 decemberében nagyjából 25 centet ért egy Bitcoin, alig három hónap múlva azonban már pontosan egy az egybe váltották a két valutát. 2011 júniusának elején egy bitérme majdnem 30 USA dollárért kelt el.[37] Ez annak köszönhető, hogy a sajtó ekkor kezdett el foglalkozni a virtuális fizetőeszközzel. Megvolt azonban a médiavisszhang árnyoldala is, hiszen az alvilág is felfigyelt a jelenségre. 2011 júniusának végén egy hackercsapat támadást indított a Bitcoin váltó *mtgox.com* ellen, aminek köszönhetően körülbelül 60.000 felhasználó feltöltött virtuális pénztárcáját lopták el. Az árfolyam emiatt meredek zuhanásba kezdett, ami egészen 2011 végéig tartott.[38] 2012-ben az árfolyam ismét emelkedésnek indult. A tanulmány írásakor egy érme körülbelül 9 USD-t ér.[39] A Bitcoin egyelőre rendkívül új jelenségnek számít az interneten, így nehéz bármit is jósolni a jövőjét illetően, mivel nem alakultak még ki stabil viselkedési minták vele kapcsolatban.

7. A piac sajátosságai: bizsuktól a kemény drogokig

Tudjuk már, hogyan működik a rendszer és azt is, hogyan juthatunk hozzá ehhez az új fizetőeszközhöz, de mégis miket vehetünk rajta magunknak? Az interneten számos honlap található, amelyeken valódi árukért, fogyasztási cikkekért vagy szolgáltatásokért fizethetünk Bitcoinnal. A paletta széles, válogathatunk ruhák, könyvek, ékszerek, számítógép alkatrészek között, és külön érdekesség, hogy van már néhány ügyvédi iroda is, amely elfogadja fizetőeszközként.[40] Ezek ártatlan és teljesen hétköznapi dolgok, viszont a Bitcoinos pénzátutalás teljes anonimitása, decentralizáltsága és lenyomozhatatlansága miatt kiváló eszköz lehet a bűnözők kezében is.



A *gawker.com* egy 2011. június 1-jén megjelent cikkében egy olyan weblapot mutatott be, amelyen keresztül bármilyen létező kábítószerhez hozzá lehet jutni.[41] A weblapot *SilkRoad*-nak hívják és csak egy különleges anonim böngészőt, a *Tor*-t használva tudjuk elérni azt.[42] Némi keresgélés és regisztráció után, azonban elénk tárul a világ legnagyobb drogpiaca, ahol a marihuánától, a heroinon keresztül az LSD-ig mindent meg tudunk rendelni. A kábítószer azonban nem minden: találhatunk itt a termesztéshez és előállításhoz szükséges eszközöket is, de rendelhetünk lőszert, szoftverlicenceket, hozzáférési kódokat különböző zárt weboldalakhoz, robbanóanyagokat és egyéb illegális, vagy épp nehezen beszerezhető termékeket. Fizetni csak és kizárólag egyetlen eszközzel lehet: Bitcoinnal.[43]

A virtuális pénz sajnos kiváló eszköz illegális célokra, hiszen szinte lehetetlen visszakövetni, hogy ki-kinek és mikor küldte a kérdéses összeget. Ettől függetlenül még véleményem szerint nem válik a virtuális érme a bűnözők pénzévé, hiszen valószínűbb, hogy csak elenyésző kisebbséget képviselnek a közösségen belül. Az anonim fizetést és a pénzmosást pedig a Bitcoin előtti időkben is megoldották az alvilágban. A Bitcoinnal, mint az online bűnözés lehetséges eszközével, a tanulmány utolsó fejezete foglalkozik részletesen.

8. Az új fizetőeszköz versenytársairól

A Bitcoinnak legalább három versenytársa van a piacon. Az első csoportba a hagyományos internetes fizetőeszközök tartoznak, amelyek az elektronikus kereskedelmet könnyítik meg, a másikba a közösségi oldalak és online játékok valutái, a harmadikba pedig a különböző államok hivatalos pénzei.

a) Az online fizetés hagyományos módjai

Az internetes fizetés egyik legelterjedtebb módszere a *PayPal* használata, amelyen keresztül igazi pénzünket utalhatjuk át a bankszámlánkról egy internetes számlára, amit használva könnyen vásárolhatunk a különböző online boltokban. Hasonló a Bitcoinhoz, viszont hiányzik belőle a decentralizáltság és a teljes anonimitás. Ennek ellenére kevésbé valószínű, hogy csupán e két tulajdonsága miatt valódi versenytársa lehet a Bitérme az internetes fizetés hagyományosabb formáinak. A legtöbb embert ugyanis nem igazán érdeklik a Bitcoin ilyen előnyei. BTC helyett euróban, vagy forintban szeretnék látni az árakat, és a legtöbben alapvetően ódzkodnak is egy teljesen új, ismeretlen valutától.[44]

Az egyetlen előnye ebből a szempontból a digitális érmének, hogy nincsenek tranzakciós költségei. Egy cikk például a külföldön dolgozó vendégmunkásokat említi, akik rendszeresen utalnak munkahelyükről haza pénzt a családjuknak. A küldemények egy részét azonban elnyelik a tranzakciós díjak, amit Bitcoint használva ki lehetne küszöbölni.[45]

b) Virtuális világok valutái

Másik érdekes terület, amivel érdemes foglalkozni a közösségi tereken, virtuális világokon belüli kereskedelem. A legtöbb online játéknak megvan a maga fizetési eszköze, amivel a játéktéren belül vásárolhatunk magunknak digitális tárgyakat. Léteznek olyan virtuális világok, ahol játékon belüli pénzünket, akár igazira is átválthatjuk, mint pl. a *Second Life*-ban[46]. A *Facebook* pedig nemrég vezette be a *Facebook-credit* rendszert, amit használva igazi pénzünket válthatjuk virtuális pénzre, amellyel a közösségi oldal olyan játékaiban, mint a *Farmville*-ben[47] vehetünk magunknak különböző javakat (például virtuális kukoricát). Az ilyen virtuális gazdaságok kifejlesztése azonban sok időt és tudást vesz igénybe, valamint nagy odafigyelést igényel a játékfejlesztők részéről. A fejlesztők pedig ugyanúgy, mint a bankok hajlamosok díjakat kérni a valuták átváltása után. Nincs ez máshogy a *Diablo III* [48] című játékban sem, ahol, ha a felhasználók a játék aukciós házában igazi dollárért szeretnének varázskardot venni kedvenc avatárjuknak, bizony számolniuk kell némi tranzakciós költséggel is.[49] A Bitcoin alapú kereskedelem éppen ezért jobb fogadtatásra számíthat a játékosközösség részéről, hiszen számukra nem idegen az, hogy fantáziavilágok kitalált fizetőeszközeiben kereskedjenek egymással, majd mindezt átváltsák igazi pénzre. A virtuális valuták mögött azonban még mindig ott vannak a játékok és közösségi hálók fejlesztői, akik igaz, hogy árgus szemmel ellenőrzik a virtuális tárgyak piacát, de biztonságot is jelentenek, hiszen az esetleges csalások esetén még mindig lehet hozzájuk fordulni.

A Bitcoin ennek ellenére jó megoldást jelenthetne egy egységes virtuális fizetőeszköz bevezetésére. A játékok fejlesztői sok időt és pénzt spórolhatnának, ha egységes valutában határoznák meg az árakat, ráadásul az átváltással sem kéne bajlódni. Erre pedig a Bitcoin, mint egységes virtuális pénz tökéletes lenne.

c) Az államok hivatalos valutái

Vajon lehet e versenytársa a Bitcoin a régi, kipróbált pénzeknek, a hagyományos bankjegyeknek, érméknek, a mögöttük álló bankrendszernek és a jogszabályokban lefektetett állami garanciáknak?

Hasonlóan az internetes utalásokhoz, a Bitcoinnak előnyei és hátrányai is vannak a hagyományos pénzzel szemben. A tranzakciós költségek minimalizálása itt is fontos tényező lehet, azonban valószínűleg jó néhány élethelyzetben nehézkes lenne az elektronikus fizetés. Ennek ellenére létezik New Yorkban egy gyorsétterem, ahol kísérleti céllal lehet már a virtuális érmével is fizetni.[50] A fizetőeszköz másik nagy hátránya pont egyik legnagyobb előnye is, nevezetesen hogy semmilyen jogi entitás nem áll mögötte, és teljesen nélkülözi a központi kontrollt. A Bitcoin átváltási értékét csak és kizárólag a kereslet-kínálat egyensúlya szabja meg, nem csoda hogy alig több mint egy év alatt egy BTC értéke a kétezerszeresére emelkedett, majd pár hónap alatt – a hackertámadások hírei miatt – a tizedére csökkent. A rendszerbe kalibrált defláció (nevezetesen, hogy egy idő után lehetetlen lesz belőle többet létrehozni), és az egyre jobban ismertté válás azonban előrevetíti az árfolyam stabilizálódását, de erre még valószínűleg várnunk kell egy kicsit.

9. Van-e a Bitcoinnak jövője?

Az országok valutái mögött megtalálhatóak az államhatalom garanciái, a Bitcoint viszont semmilyen jogi entitás nem biztosítja. A tények ennek ellenére azt mutatják, hogy mégis van kereslet az új virtuális valutára, és megbíznak a rendszerben azok használói. Az alábbi eset kiválóan szemlélteti, hogy lehet létjogosultsága egy ehhez hasonló pénznek.

Reuben *Grinberg* egy 2011-es tanulmányában az iraki „svájci dinárhoz" hasonlította a Bitcoint, mivel a történelem során ez volt az egyetlen olyan fizetőeszköz még, amely mögött sem állami garancia nem állt, sem áruval, nyersanyaggal (pl. arannyal) nem volt biztosítva és ennek ellenére mégis több mint egy évtizeden keresztül fent maradt a piacon.

Irakban az 1991-es öbölháborút követő években sajátos helyzet alakult ki. A bankjegyeket a háború előtt (svájci nyomólemezekkel) Angliában gyártották, a háború utáni embargó miatt azonban ez a lehetőség megszűnt, így helyileg, illetve Kínában készültek a bankjegyek. Az új bankjegyek silány minőségűek voltak, ezért a pénzhamisítás elharapódzott, a hamisítványok nem ritkán jobb kivitelűek voltak, mint az eredetiek. A háború következtében az ország északi részén elterülő, autonóm Kurdisztán a harcokat követően de facto függetlenné vált, habár ezt de jure sosem nyilatkoztatta ki. Itt az új, gyenge minőségű bankjegyeket nem fogadták el, hanem az addigra Irak többi részében forgalomból kivont régi papírpénzeket használták tovább. A két pénzrendszer árfolyama hamarosan eltávolodott egymástól, ezzel lényegében új pénznem jött létre, melyet iraki „svájci dinár" néven emlegettek. Ennek a valutának se központi bankja, se hivatalos árfolyama, se bármiféle garancia az értékére (arany- vagy valutatartalék) nem volt; mivel azonban új pénzeket se nyomtattak, értékéből nem vesztett, sőt a bankjegyek kopása miatt inkább enyhe defláció volt jellemző.[51] Irak 2003-as amerikai megszállása után az Amerikai Egyesült Államok által támogatott átmeneti kormány új pénzt veretett és lehetővé tette, hogy át lehessen váltani a kurd területen forgalomban lévő svájci dinárt az új valutára. Ekkor 1 svájci dinárért 150 új dinárt adtak. Ez a példa jól szemlélteti, hogy fent tud maradni egy olyan valuta, mely mögött nem állnak garanciák, ha a piac, mint fizetőeszközt elfogadja azt és megbízik benne.[52]

Ez a bizalom azonban több okból kifolyólag is meginoghat a jövőben. Sokan azért bíznak a Bitcoinban, mint fizetőeszközben, mivel a központi kontroll hiánya miatt nem lehet mesterségesen gerjeszteni az inflációt. Azonban előfordulhat, hogy valamilyen külső csoport hatására ez mégis bekövetkezik. Erre jó példa a már említett Mt.Gox elleni hackertámadás, aminek hatására hiperinfláció következett be. Sokan pont emiatt veszíthetik el a virtuális pénzbe vetett bizalmukat.

Továbbá bizonytalanná teheti a Bitcoin jövőjét az is, hogy idővel kialakulhatnak versenytársai is. Mivel a szoftver nyílt forráskódú, semmilyen akadálya nincs annak, hogy valaki továbbfejlessze azt, és esetleg kialakítson egy új, jobban működő fizetőeszközt. Igaz, ez nem tűnik valószínűnek, mivel logikus hogy az újításokat inkább a már meglévő Bitcoin szoftver fejlesztésére használják, de ettől még számolni lehet a bekövetkezésével.

A bizalom elvesztésével járhat az is, ha elharapódznak a lopások. Mivel az anonim tranzakciós rendszer miatt csak nagyon nehezen lehet követni az utalásokat, egy ilyen lopás akár egy felhasználó teljes Bitcoin vagyonának elvesztésével járhat. A Bitcoin-tolvaj utáni nyomozás járhat ettől még sikerrel, de az átutalások nehézkes követése miatt sokkal időigényesebb is lesz az.

Ezen kívül elveszítheti sokak szemében még a Bitcoin az értékét azon tulajdonsága miatt is, hogy csak a világhálón létezik. Ha nincs internetkapcsolatunk, akkor Bitcoinunk sincs, hiába van ott a virtuális pénztárcánk a gépünkön, magát a fájlt nem tudjuk pénzzé tenni sehogy. Ma már elég valószínűtlen hogy a világon mindenhol, de legalábbis közvetlen környezetünkben huzamosabb időre megszakad az internetkapcsolat, minden esetre ez is megalapozhatja a bizalomvesztést és a valuta elértéktelenedését.

Összegzésképpen elmondható, hogy a Bitcoint decentralizált és biztosítatlan volta nem ítéli automa-

tikusan halálra, viszont a felhasználóknak számolniuk kell azzal, hogy ez az új, még fejlődésben lévő fizetőeszköz akár meg is bukhat a jövőben.

10. A Bitcoin jogi státuszáról

A Bitcoin jogi státuszára jelenleg csak annyi biztosat lehet mondani, hogy abszolút nincs szabályozva sehol a világon. Az ellenőrizhetetlen, teljesen független virtuális fizetőeszköz tulajdonságaiból adódóan minden eddigi törvényi szabályozást kikerül és egyfajta jogi „szürke zónában" helyezkedik el. A hatályos törvényi szabályozást felhasználva megpróbálom áttekinteni, hogy jogilag hogyan lehet értékelhető a Bitcoin-jelenség.

a) A Bitcoin mint pénz

Kérdéses lehet, hogy vajon az államok betilthatják-e a Bitcoint, mint pénzt. A világon a legtöbb országban a pénzkibocsátás jogával kizárólagosan az állam központi bankja rendelkezik.

Az Amerikai Egyesült Államokban 1837 és 1866 közötti időszakot az ún. „szabad bank korának" nevezzük, mivel csaknem bárki saját magánpénzt adhatott ki ezért több, mint 8000 különböző pénz volt forgalomban. Ha a kibocsátó tönkrement, bezárt, elköltözött vagy akármi más módon felfüggesztette tevékenységét, az általa kibocsátott pénz egyszerűen értéktelenné vált. Ennek a gyakorlatnak az 1863-as Nemzeti Bank Törvény vetett véget, amely betiltotta a magánpénzek kiadását.[53] Sok más nemzetnél is alkalmaznak hasonló módszereket, hogy korlátozzák a magánszektor kormányzattal való versengését. Ennek megfelelően a pénzkibocsátás kizárólagos jogával hazánkban a Magyar Nemzeti Bank rendelkezik.[54] A Bitcoinnak azonban a magánpénzekkel ellentétben nincs hivatalos, központi kibocsátója, hanem azt a felhasználók állítják elő a számítógépeik segítségével. Bárki, aki bányász-szoftvert futtat, vagy tagja egy bányás-társulásnak tulajdonképpen Bitcoin kibocsátó is egyben. Mivel szerte a világon állítanak elő így az új fizetőeszközből, lehetetlen lenne adott állam számára, hogy effektíven megtiltsa az előállítását, ha csak nem lenne ellene nemzetközi fellépés, ami a bányászat betiltásával ellehetetlenítené a virtuális valuta helyzetét.

Ilyen pénzbetiltási akciónak lett áldozata az ún. *Liberty Dollár* is, amelyet 1998 és 2011 között állított elő Bernard *von NotHaus* az USA-ban, aki azért fejlesztette ki ezt az alternatív fizetőeszközt, hogy ne legyen kitéve a dollár inflációjának.[55] Többen is használták a Liberty Dollárt, ami egy idő után szemet szúrt az USA kormányának és végül be is tiltották azt, mint megtévesztő fizetőeszközt. A Bitcoinnal ellentétben azonban ez a valuta biztosítva volt aranynyal, ezüsttel és már értékes fémekkel, ráadásul papír és érme formában jelent meg a piacon úgy, mint az egyes államok hivatalos valutái.[56] Az ítélet indoklása szerint a tiltás nem a magánpénzek elleni támadásként értékelendő, hanem a csalás és pénzhamisítás megelőzését kívánja segíteni.[57]

A fentiek alapján megállapítható, hogy a Bitcoin nem sorolható be a klasszikus valuták közé, mivel az említett tulajdonságai miatt nem lehet rá alkalmazni a jogszabályokat. Lehet esetleg máshogy értékelni, például valamilyen értékpapírként, vagyoni értékű jogként, egyfajta sajátos szellemi termékként vagy árucikként?

b) A Bitcoin mint értékpapír

Értékpapírnak csak olyan okirat vagy – jogszabályban megjelölt – más módon rögzített, nyilvántartott és továbbított adat tekinthető, amely jogszabályban meghatározott kellékekkel rendelkezik és kiállítását (kibocsátását), illetve ebben a formában történő megjelenítését jogszabály lehetővé teszi.[58] Mivel az értékpapír adat is lehet, felmerülhet a kérdés, hogy vajon tekinthető-e annak a Bitcoin.

Az értékpapírfajtákon belül, leginkább a részvényekkel hasonlítható össze a virtuális érme. Egy adott részvénytársaság adott részvényei – fajtától függően – teljesen egyneműek, és ez lehetővé teszi, hogy központosított piacokon (értéktőzsdéken) kereskedhessenek velük, vagy a társaság tagjai adják-vegyék egymás között. A Bitcoinok is így viselkednek, hiszen azokkal csak egy zárt rendszert használva tudunk fizetni egymás között. Ezzel szemben a jelenlegi jogszabályok megkövetelik, hogy részvényt csak részvénytársaság bocsáthat ki. A Bitcoinokat pedig nem gazdasági társaságok, hanem a felhasználók hozzák létre a decentralizált hálózaton.

Egy részvény tagsági és egyéb jogokat (pl. szavazati jogot) testesít meg adott társaságon belül.[59] Egy Bitcoin birtoklásához nem kapcsolódnak ilyen jogok, mivel azok mögött nem áll semmilyen jogi személy. A részvénytársaság előre meghatározott számú és névértékű részvényekből álló alaptőkével (jegyzett tőkével) alakul, a tag (részvényes) kötelezettsége pedig a részvénytársasággal szemben a részvény névértékének vagy kibocsátási értékének szolgáltatására terjed ki.[60] A Bitcoin rendszer létrehozásakor azonban alaptőkéről nem beszélhetünk, hiszen az érmék mögött nincs fedezet, hanem azokat számítógépek és elektromos áram segítségével, matematikai problémák megoldásával hozza létre a hálózat gyakorlatilag a nulláról indulva.

Az értékpapírokra vonatkozó általános szabályok szerint az értékpapír kiállítója (kibocsátója) feltétlen és egyoldalú kötelezettséget vállal arra, hogy ő maga vagy az értékpapírban megnevezett más személy az értékpapír ellenében meghatározott pénzösszeget szolgáltat az értékpapír jogosultjának.[61] A Bitcoin azonban nem váltható át előre meghatározott pénzösszegre senkinél sem, hiszen annak nincs kibocsátója. Az más kérdés, hogy léteznek egyes internetes szolgáltatások, melyek arra vállalkoznak, hogy átváltják a bitérméket való-világbeli valutákra. Ez azonban nem más, mint egy egyszerű adás-vételi szerződés, amelyben az egyik fél virtuális fizetőeszközt vesz valutáért cserébe.

c) A Bitcoin mint vagyoni értékű jog

Egy jogalany vagyonán belül aktív és passzív vagyont különböztetünk meg. Az aktív vagyon egyes elemei a vagyontárgyak, mint a dolgok, vagyoni értékű egyéb jogok és követelések.[62] Vagyoni értékű egyéb jognak tekinthetők a pénzben kifejezhető értékű jogok, mint például földhasználati jog, haszonélvezeti jog, bérleti jog, szellemi alkotások felhasználási joga, vagyonkezelői jog.

A felhasználók által birtokolt Bitcoin mennyiség feletti rendelkezési jog vagyoni jellegű jogként történő értékelése számos kérdést vethet fel, különösen, ha mint valaki szellemi alkotását vizsgáljuk, amelyhez kapcsolódhat felhasználási jog. A hálózaton létrehozott érmemennyiséget azonban nem tekinthetjük senki szellemi alkotásának, mivel a blokkokat a felhasználók számítógépei hozzák létre matematikai algoritmusok megoldásával. A magyar szerzői jogi törvény és a nemzetközi joggyakorlat szerint a matematikai művelet nem lehet tárgya szerzői jogvédelemnek.[63] Létrehozása pillanatában a Bitcoin használati joga azt illeti meg, akinek a gépe megoldotta az adott problémát. A rendszer természetéből adódóan a Bitcoinnak eredendően nincs tulajdonosa és nem tekinthető szellemi terméknek sem, mivel csak egy adatsor a számítógépen a virtuális pénztárca fájlban, melyet matematikai műveletek hoztak létre, ezért hozzá vagyoni értékű jog nem kapcsolódhat. Egy Bitcoin mennyiség mindenkori használójának egyszerűen azt kell tekinteni, akinek a birtokában van a pénztárca fájl.

d) A Bitcoin mint szellemi termék

Érdekes szemléletváltás lehet, ha nem magából a fizetőeszközből indulunk ki, hanem a fájlból, ami tartalmazza azt, és amin keresztül hozzáférhetünk.

A wallet.dat névre hallgató pénztárcafájl a felhasználók számítógépein található a merevlemezen. Funkciója az, hogy tartalmazza az egyes Bitcoinok hozzáféréséhez szükséges nyilvános és privát kulcspárokat. A pénztárcafájl minden egyes felhasználónál egyedi, nem találkozhatunk két egyformával. Lehetséges lemásolni, de ez nem duplázza meg a birtokunkban lévő Bitcoin mennyiséget. A felhasználó, amikor tranzakciós műveletek végez, folyamatosan változtatgatja a virtuális pénztárca fájl tartalmát. Ennek ellenére nem tekinthető ez a fájl a felhasználó szellemi termékének, mivel a szerzői jog csak a szerző magasabb rendű szellemi tevékenysége által létrehozott alkotásokat részesíti védelemben, a pénzátutalás pedig nem tekinthető annak.

Ezek alapján a wallet.dat-ra nem terjed ki a szerzői jog, azt nem lehet a felhasználók szellemi tulajdonának tekinteni. Ez csak egy olyan fájl a számítógépen, mely birtokolható, használható, másolható és tetszés szerint változtatható, de csak a Bitcoin kliens szoftveren keresztül.

e) A Bitcoin mint árucikk

A Bitcoin olyan árucikként való értékelése, amin tulajdonjog szerezhető szintén lehet kiindulási pont. Felfogható, hogy az áram és a computerek számítási képességének felhasználásával egyfajta termékként jön létre, melyet aztán átcserélhetünk más árucikkekre a virtuális piacon. Ez az elmélet azonban nem veszi figyelembe, hogy alapvetően fizetőeszközként viselkedik a Bitcoin és nem valamilyen más fogyasztási cikként.

A virtuális fizetőeszköz annak ellenére, hogy a jelenlegi törvények alapján nem igazán lehet sehová besorolni, még mindig a pénzhez áll legközelebb. A polgári jogi dogmatikai alapján a pénz dolognak minősül és azon tulajdonjog szerezhető.[64] Mivel a felhasználók fizetési eszközként használják a Bitcoint, és annak viselkedése leginkább a pénzhez hasonlít érdemes ekként viszonyulni hozzá és egy sajátos analógiával élve dolognak tekinteni azt. A szokás is azt alakította ki, hogy az emberek pénzként tekintenek a Bitcoinra, és érvényes csereeszközként fogadják el azt a piacon. Sajnos a fentiek alapján a törvényi szabályozás nem volt felkészülve egy ilyen találmányra, ezért jelenleg a Bitcoin jogi státusza nem szabályozott semmilyen formában.

11. A Bitcoin mint a bűnözés lehetséges eszköze

Mint már arra az előzőekben is tettem utalást az anonim módon használható pénz kiváló eszközül szolgálhat alvilági célok megvalósítására. A témával nem csoda, hogy az elmúlt időszakban a bűnüldöző

hatóságok is elkezdtek foglalkozni, az FBI például terjedelmes belső jelentésben taglalta rendszer működését, amely az internetre is kikerült időközben.[65] A témával érdemes ezért ebből is szemszögből külön is foglalkozni, mivel első ránézésre az anonim pénzátutalási lehetőséget a pénzmosás melegágyának lehet tekinteni a lenyomozhatatlansága miatt. Vajon tényleg olyan nehéz feladatok elé állítatja az igazságszolgáltatást az új fizetőeszköz megjelenése, mint amilyennek elsőre tűnik? Mik a rendszer veszélyei és hogyan lehetne megelőzni a károk bekövetkezését? A következő fejezetben többek között ezekre a kérdésekre keresem a választ.

a) A központi kontroll hiányának veszélyei és előnyei

A Bitcoin hálózat azon sajátossága miatt, hogy a felhasználóknak nem kell semmilyen adatot megadniuk a szoftver használata során, valamint a központi felügyelő szerv hiányából következőleg az esetleges gyanús tranzakciók kiszűrése, az egyes felhasználók azonosítása és a tranzakciós naplók beszerzése első ránézésre lehetetlen vállalkozásnak tűnhet.

Sok olyan tulajdonsága van azonban a rendszernek, amely mégis megkönnyítheti az egyes tranzakciók azonosítását, és azok konkrét személyekhez kötését. Az első, hogy a Bitcoin decentralizált rendszerében minden egyes tranzakció nyilvános, és bárki által megtekinthető a *www.blockexplorer.com*, vagy a *http://blockchain.info* honlapon keresztül.[66] Nem kell tehát a virtuális pénzzel történő átutalások követése érdekében adatlekéréssel fordulnunk semmilyen hatósághoz, vagy pénzintézethez, hiszen azokat mi is bármikor szabadon megtekinthetjük. Egy bizonyos gyanús Bitcoin címről ezek alapján végigkövethető minden egyes utalás, amelyet a világhálón keresztül végrehajtottak.

Ez azonban még sajnos nem garancia arra, hogy azonosítani tudjuk az anonim tranzakciós-lánc mögötti személyt, aki a pénzösszeget a különböző címek között mozgatja, hiszen a blokk-láncban sem lelhető fel semmilyen különösebb információ azon kívül, hogy mennyi Bitcoint, melyik címre utaltak át.

Ebből a szempontból segítségünkre lehet, ha szem előtt tartjuk, hogy a Bitcoint egyelőre inkább egyfajta internetes fizetést egyszerűsítő és anonimizáló eszközként kezelik a cybertérben, nem pedig a valódi fizetőeszközöket helyettesítő pénzként. Ez alatt azt értem, hogy a felhasználók jellemzően egy bizonyos cél érdekében vesznek maguknak Bitcoinokat (például egy webáruházban való vásárlás okán), majd előbb-utóbb visszaváltják azokat a fizikai világban is használható pénzre.

Mint ahogy arról az előző fejezetekben már szó esett, az egyes országok hivatalos valutáit néhány erre specializálódott devizatőzsde honlapon lehet Bitcoinra váltani és vissza. Ilyen a már többször említett japán székhelyű *Mt. Gox* is *(http://mtgox.com)*. A honlapon elérhető szolgáltatások igénybevételéhez regisztrálniuk kell az egyes felhasználóknak, amely során elég megadni egy felhasználónevet, jelszót, valamint e-mail címet. Ennyi adat első ránézésre nem tűnik túl sok információnak adott személyről, azonban azok alapján már el lehet indulni a további azonosítás útján. A honlap üzemeltetői esetleg választ tudnak arra adni, hogy egy bizonyos Bitcoin címet használó személy regisztrált-e a portáljukon, ha igen milyen felhasználónevet és e-mail elérhetőséget adott meg, illetve milyen IP címeket[67] használva jelentkezett be a profiljába. Léteznek olyan szolgáltatók is, amelyek bankszámlaszámok megadását kérik az egyes felhasználóktól, hogy később az átváltott összeget erre tudják utalni. Az esetleges bankszámla forgalmi adatai, valamint megnyitása során keletkezett dokumentumok már általában elegendő információt tartalmaznak egy adott személy azonosításához. A FBI jelentése szerint továbbá szintén kiindulási pont lehet a címeiket különböző internetes fórumokon közzétevő felhasználók hozzászólásainak vizsgálata.

b) Pénzmosás virtuális elszámolási egységekkel

A Bitcoin az anonim fizetési lehetőség, és a gyakorlatilag nullával egyenlő tranzakciós költségek miatt ideális eszköznek tűnhet a bűncselekmények elkövetéséből származó pénzösszegek elrejtésére, a pénzek „tisztára mosására". Az FBI elemzése szerint ez a feltételezés abból fakadhat, hogy más virtuális elszámolási egységekkel is történtek már hasonló cselekmények egyes bűnügyek kapcsán. Ezek a virtuális valuták lehetnek egyszerű elektronikus fizetési egységek, amelyekkel honlapokon vásárolhatunk magunknak különböző fogyasztási cikkeket (pl. *WebMoney*), vagy online játékok virtuális pénzei (pl. a World of Warcraft online szerepjátékban használt aranytallérok).

Erre példa az a klasszikus eset is, amelyben egy internetes szervezett bűnözői csoport egy online szerepjáték virtuális valutájára váltotta át egy erre specializálódott honlapon a bűncselekmények elkövetéséből származó valódi pénzét, majd a játék piacán eladásra kínált virtuális tárgyakat vett, és ezeket a játéktárgyakat később tovább értékesítette a többi játékos számára, de immár valódi „tiszta" pénzért.[68] A népszerűbb online szerepjátékok virtuális piacain használt elszámolási egységeket általában erre specializálódott különböző külsős honlapokon lehet igazi pénzre váltani. Léteznek olyan virtuális

világok is, ahol viszont kifejezetten a játékfejlesztők építették be a virtuális pénz valódira történő váltásának lehetőségét a játékba, és fordítva (például a Second Life élet-szimulátor, vagy a Diablo III fantasy szerepjáték).

Visszatérve az eredeti témára a pénzek Bitcoinra történő átváltásával, majd annak különböző Bitcoin-címekre való továbbutalgatásával elvileg könnyen megvalósítható a bűncselekmények elkövetéséből származó pénzösszegek tisztására mosása. Mivel azonban a tranzakciók nyilvánosak és naplózva vannak az interneten a közeg rendelkezésre áll a gyanús átutalások feltérképezésére. A központi Bitcoin váltó honlapokon történt BTC-valós pénz cserékről is rendelkezésre állhatnak különböző információk, amelyeket a weboldalt üzemeltető cég kezel.

Nehézségeket okozhat a különböző Bitcoin-váltó honlapok üzemeltetőinek elérése a nyomozóhatóságok részéről, ha azok nem egyazon országban tevékenykednek. Vegyük például, hogy egy magyarországi hatóság szeretne valamilyen Bitcoin cím felhasználójáról információkat szerezni az mtgox.com-on üzemelő Bitcoin-tőzsdétől. A honlapot fenntartó *Tibanne Co. Ltd.* nevű társaság Japánban került bejegyzésre, és innen is üzemelteti a honlapot.[69] A Japán (és egyébként szinte minden külföldi) hatóságoktól általában csak hivatalos jogsegélykérelmi eljárás keretében lehetséges a büntetőeljárás során ilyen adatokat bekérni, amely a fordítási munkálatok és elbírálás miatt akár hosszabb időt (több hónapot) is igénybe vehet. Ezen eljárás szabályairól a nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény rendelkezik. A hivatalos jogsegélykérelem teljesítésének ideje alatt lehetséges, hogy a kérdéses logadatokat (pl. a profilba történő bejelentkezések IP címei) a cég már törölte az adatbázisából. Célszerű lenne emiatt egy online felületet biztosítania a kisebb-nagyobb Bitcoin-váltó honlapoknak, ahol egyszerűbben és gyorsabban lehet ilyen hatósági adatkérésekkel hozzájuk fordulni (pl. központi e-mail cím, visszaélés bejelentő felület stb.). Sajnos ez jelenleg még egyáltalán nem jellemző a váltó-honlapokra.

Szintén további nehézségeket okozhat, ha a különböző váltók olyan országokba jegyeztetik be a székhelyüket, amelyeket nem kötelez adatszolgáltatási kötelezettség nemzetközi szerződés alapján. Eddig nem jellemző, hogy a Bitcoin-váltásra szakosodott cégek kifejezetten ilyen offshore központoknak minősülő helyekre helyezik át a székhelyüket, minden esetre érdemes a jövőben számolni ezzel a lehetőséggel is.

Nehezítheti a helyzetet, ha az átváltás nem az interneten, hanem egyszerűen a valós pénz kézbe történő átadásával történik, vagy ha különböző Bitcoin címeken található összeget egyesítenek egy közös címen, illetve ha egy közös nagyobb összeget tartalmazó címet bontanak fel kisebbekre.

Az interneten találhatóak továbbá olyan speciális honlapok, amelyek nem titkoltan Bitcoin-mosásra szakosodnak, az egyes felhasználók anonimitásának megőrzése érdekében. Ilyen a *http://bitcoinlaundry.com/* is, ami egy központi Bitcoin címet takar, ahová szabadon átutalhatjuk virtuális érméinket, majd onnan – némi tranzakciós díj ellenében – egy általunk megadott címre utalja azt tovább az üzemeltető.[70]

c) Bitcoin lopás

Mivel a Bitcoin meghatározott értéket képvisel az interneten, számolni kell annak a valószínűségével, hogy egyesek el szeretnék lopni a tulajdonosoktól, a fizikailag létező pénz alternatívájára. A pénzmosással ellentetében Bitcoinok ellopásáról már konkrét eseteket is dokumentál a szakirodalom és a média, így valószínűleg nagyobb arányban lehet majd ilyen típusú visszaélésekre számítani a jövőben.

Az efféle visszaélések szempontjából a legfontosabb tényező a számítógépen található virtuális pénztárca fájl (wallet.dat), ami dokumentálja, hogy épp mennyi virtuális érme felett rendelkezhetünk. Ha letöröljük számítógépünkről ezt a fájlt – és nem készítettünk róla semmilyen biztonsági másolatot – végérvényesen elveszíthetjük hozzáférésünket a pénzünkhöz. Ilyenkor a Bitcoinok nem törlődnek ki a rendszerből, „csupán" azokat a nyilvános és privát kulcspárok nem lesznek a birtokunkban, amik a hozzáférést biztosítják hozzájuk. Mint már az előző fejezetben kitértem rá, a Bitcoin törvényi besorolását tekintve jelenleg egyfajta jogi „szürke zónában" helyezkedik el. Viselkedését tekintve viszont leginkább a pénzhez hasonlít, így véleményem szerint javasolt így tekinteni rá a joggyakorlatban.

Mivel a magyar polgári jog szabályai szerint[71] a pénz dolognak minősül, a Büntető Törvénykönyvről szóló 1978. évi IV. törvény (továbbiakban: Btk.) 316. §-ában szabályozott lopás bűncselekményt pedig csak olyan értékekre lehet elkövetni, amelyek dolgoknak minősülnek, így magyarországi viszonylatban a Bitcoinnal történő vagyon elleni visszaélésekre is a lopás törvényi tényállását kellene alkalmazni. Ez azonban sok problémát okozhat, mivel a Bitcoin kétes jogi besorolása miatt sokszor nehéz lenne a bűncselekmény kétséget kizáró minősítése. Előfordulhat, hogy egy-egy Bitcoinnal való vagyon elleni bűncselekményre jobban ráillik a Btk. 318. §-ában szabályozott csalás, vagy a 300/C. § szerinti számítástechnikai rendszer és adatok elleni bűncselekmény, illetve a 300/E. § szerinti számítástechnikai rendszer védelmét biztosító technikai intézkedés

kijátszása, esetleg ezek halmazata. Ilyenkor az eset összes körülményeit mérlegelve kell kiválasztani a pontos minősítést.

Mivel a számítógépes környezet elengedhetetlenül szükséges a Bitcoinnal való bűncselekmények elkövetésére, így – noha az tulajdonságait tekintve inkább pénzként, tehát dolog módjára viselkedik, mint adatként – indokolt lehet a virtuális pénzlopásokat inkább számítógépes bűncselekményként (tehát a Btk. 300/C. §, vagy a Btk. 300/E. §-aiba ütköző magatartásokként) értékelni, mint lopásként. Ez a kényszerű minősítés azonban leginkább a törvényi szabályozás idejétmúltságából fakad. Örvendetes lenne a virtuális pénzekkel, virtuális tárgyakkal elkövetett visszaélések értékelésének rendezése a jövőben.

Néhány példát nézve, az egyik legfeltűnőbb és legnagyobb sajtóvisszhangot kiváltó esemény a már többször említett Mt. Gox pénzváltó honlap elleni hackertámadás, ami során számos Bitcoin-használó virtuális pénztárcáját lopták el. Ha ezt a bűncselekményt szeretnénk a hatályos magyar jogszabályok alapján minősíteni, akkor először semmiképpen sem a lopás, hanem a Btk. 300/C. § szerinti, meghatározott kárt okozó számítástechnikai rendszer és adatok elleni bűncselekmény lenne a helyes besorolás. A törvényszöveg szerint az követi el a büntetendő cselekményt, aki számítástechnikai rendszerbe a számítástechnikai rendszer védelmét szolgáló intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága kereteit túllépve, illetőleg azt megsértve bent marad. A hackerek a Bitcoin-váltó honlap biztonsági hiányosságait kifürkészve és kihasználva törtek be a rendszerbe és szerezték meg ott tárolt adatokat, tehát a felhasználók virtuális pénztárcáit.

Egy másik eset szerint 2011 júniusában kezdett el kéretlen e-mailek (spamek) útján terjedni egy trójai vírus, amely nem csinált mást, mint a gyanútlan áldozatok számítógépére települve a wallet.dat nevű fájl alapértelmezett elérési útvonalát használva megpróbálta azt elküldeni egy lengyelországi szerverre a vírus írójának.[72] Az *Infostealer.Coinbit* névre hallgató vírus primitívsége miatt azonban nem jelentett túl nagy veszélyt a Bitcoin tulajdonosokra, mivel csak az alapértelmezett elérési útvonalát ismerte a wallet.dat-nak, ráadásul egy egyszerű tűzfal is nehézségek nélkül blokkolta az akciót, amikor az megkísérelte elküldeni a fájlt az interneten keresztül. A vírus írójának jogi felelősségére a magyar jog szerint a Btk. 300/E. § szerinti számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása bűncselekmény tényállásában meghatározottak lehetnek irányadóak. A tényállás szerint, a bűncselekményt az követi el, aki a Btk. 300/C. §-ban meghatározott bűncselekmény elkövetése céljából, az ehhez szükséges vagy ezt könnyítő számítástechnikai programot, jelszót, belépési kódot, vagy számítástechnikai rendszerbe való belépést lehetővé tevő adatot készít. Ha a vírusprogramnak sikerül elküldeni a kérdéses fájlt a cyberbűnöző részére, akkor neki természetesen már nem csak a Btk. 300/E. §-ben, hanem a 300/C. §-ban meghatározott bűncselekmény elkövetéséért is felelnie kell.

Kifinomultabb módszer lehet, ha nem közvetlenül a már létrehozott Bitcoinokat szeretnék ellopni a tulajdonosaiktól, hanem számítógépeket akarnak befogni az interneten keresztül további érmék bányászására, egyfajta Bitcoin-termelő zombihálózatot felépítve, a résztvevő gépek tulajdonosainak tudta és beleegyezése nélkül.[73] Az ilyen illegális célokra kiépített hálózatokat botneteknek nevezzük.[74] Ehhez először a cyberbűnözőnek el kell érnie, hogy áldozata számítógépére egy olyan vírusprogram települjön, amely aztán Bitcoin bányászásra használja fel a célgép processzorának és videokártyájának számítási képességeit. Ezt legegyszerűbben elektronikus úton terjedő kéretlen reklámlevelek útján (*spamek*), vagy adathalász honlapok létrehozásával lehet elérni. Ha a sértett véletlenül kéretlen e-mailekben elhelyezett hivatkozásokra kattint, vagy olyan káros honlapokat látogat, ahol adatokat kell megadnia (pl. e-mail cím, Facebook profil és ezekhez kapcsolódó jelszavak), az internetes linkek útján terjedő vírus egyszerűen be tud férkőzni a számítógépébe.

Példa erre a jelenségre az úgy nevezett *ZeUs* néven terjedő malware vírus, amely a számítógépre települve Bitcoin bányászásra használja fel annak erőforrásait. Ez a káros szoftver különböző internetes közösségi oldalakon elhelyezett megtévesztő reklámokon keresztül terjedt 2011 első félévében.[75]

Más források megemlítik, hogy szintén kedvelt célpont lehet cyberbűnözői körökben különböző nagyobb számítógép-hálózatok (pl. egy egyetem, vagy egy cég hálózata) elleni támadás, és ehhez kapcsolódó gépek befogása együttes bányászásra. Ez azért is lehet célszerűbb megoldás, mivel a hatékony Bitcoin-termelés jellemzően rendkívül nagy számítókapacitást igényel.[76] A fenti cselekmények büntetőjogi minősítésére is a Btk. 300/C., illetve a 300/E. szakaszai irányadóak, tekintettel arra, hogy a káros programok akadályozzák a számítógépes rendszer működését, továbbá a vírusprogram terjesztését önmagában is büntetendő cselekményként értékeli a törvény.

A fenti problémákkal foglalkozik többek között az Európai Bizottság C7-0293/10 számú javaslata, amely az információs rendszerek elleni támadások jogszabályi hátterének közösségi harmonizálásra fogalmaz meg üdvözlendő javaslatokat, különösen hogy a számítógépes bűncselekmények elkövetéséhez

botnet zombihálózatok létrehozása és felhasználása súlyosító körülményként kellene, hogy megjelenjen a tagállamok büntetőjogi szabályozásaiban.[77]

d) A Bitcoin felhasználása egyéb illegális tevékenységekhez

A Bitcoin, mint anonim módon használható virtuális valuta kedvelt eszközként szolgál az interneten különböző illegális termékek beszerzésére is. A már említett klasszikus példa erre a *SilkRoad* nevű anonim piac, ahol kifejezetten törvény által tiltott, vagy nehezen beszerezhető, illetve engedélyköteles árukat lehet vásárolni a többi regisztrált felhasználótól, úgymint kábítószerek, fegyverek, lőszerek stb.

A számítógépes bűnözés tendenciái is azt mutatják, hogy a kifinomultabb módszereket alkalmazó hackercsoportok is előszeretettel használják a Bitcoint fizetőeszközként. Ilyen például a *LulzSec* internetes szervezet, amelynek egyik tagja Bitcoint használt egy botnet program felvásárlására. A *LulzSec* továbbá különböző internetes fórumokon közzétette, hogy eddig csaknem 18.000 USD-nek megfelelő összeget kapott Bitcoinban különböző felajánlások révén, amelyeket támogatóik utaltak át számukra.[78]

e) A Bitcoin rendszer, mint piramisjáték

Kevésbé kapcsolódik a fenti problémákhoz, de mindenképpen érdemes szót ejteni arról, hogy egyes kritikusai szerint a Bitcoin-jelenség nem egyéb egy világméretű piramisjátéknál, amely csupán a tervezők és az első néhány érmetulajdonos érdekeit elégíti ki és jelent számukra tetemes anyagi bevételt. A későbbi belépőknek pedig inkább ráfizetéses üzlet a virtuális valutába fektetés és azzal való kereskedés.[79]

A piramisjáték szervezése a csalás speciális formája, amelynek lényege, hogy a játékba beszállók megadott összeget fizetnek a láncban felettük állóknak, és ha sikerül rávenni ugyanerre néhány ismerősüket, akkor a befizetett pénz többszörösét nyerhetik vissza különböző újraelosztási szabályok szerint. Egy egyszerű matematikai számítással hamar kiderül, hogy a játék csak azoknak fog jelentős nyereményt hozni, akik elkezdik. Minél később száll be valaki, annál nagyobb a valószínűsége annak, hogy végleg elveszíti a pénzét.[80]

A piramisjáték szervezői természetesen azt hangoztatják, hogy a befizetésekkel mesés vagyonra lehet szert tenni, az egyáltalán nem kockázatos és egyfajta üzleti, marketing rendszerként tüntetik fel azt. A valódi piramisjátékokban a szervezők a további beszervezetteknek azt ígérik, hogy azok is profitálni fognak a játékban való részvételből. A játékok további jellemzője, hogy azok csupán a tagok pénzbefizetéseiből tartják fent magukat, a játékosok a befizetett összegek után pedig általában semmilyen valós szolgáltatást vagy terméket nem kapnak.

A piramisjátékok szervezését a magyar jog is büntetni rendeli, szabályozása a Btk. 299/C. §-ában található meg. A törvényi tényállás szerint, aki mások pénzének előre meghatározott formában történő és kockázati tényezőt is tartalmazó módon való összegyűjtésén és szétosztásán alapuló olyan játékot szervez, amelyben a láncszerűen bekapcsolódó résztvevők a láncban előttük álló résztvevők számára közvetlenül vagy a szervező útján pénzfizetést vagy más szolgáltatást teljesítenek, bűntettet követ el, és három évig terjedő szabadságvesztéssel büntetendő.[81]

A Bitcoin-rendszer piramisjátékként való értékelése mellett kevés érv szól. A legfőbb az, hogy a virtuális fizetőeszközben korán fantáziát látó, vagy azzal kísérletező kevesek könnyen tudtak gyorsan nagy összegekhez jutni, hiszen a Bitcoin-hálózat indításának elején még kevés bányász dolgoztatta számítógépét, és a hálózat szabályai szerint egy Bitcoin-blokk előállításának nehézsége arányosan nő, minél több számítógép csatlakozik a hálózathoz azért, hogy virtuális pénzt állítson elő.[82] A korai felfedezők tehát mára akár milliomosokká válhattak egy egyszerű otthoni PC-t használva, ma pedig külön szerverek léteznek külön erre a célra kialakított számítógépekkel a bányászásra.[83]

A Bitcoin rendszerből való profitálás a piramisjátékoktól eltérően nem arra épül, hogy a korai belépők a rendszer népszerűsítés útján történő kiszélesítésével és új tagok beléptetésével minél több pénzt szedjenek be a későbbi tagoktól. A korai Bitcoin tulajdonosok a virtuális valuta árfolyamának növekedéséből tettek szert nyereségre.[84] A valós pénzükön Bitcoinokat vevők minden esetben ellenszolgáltatásként virtuális pénzt kapnak, amelyet elkölthetnek különböző termékekre, vagy visszaválthatnak más valutákra.

A Bitcoin vásárlások mögött valós gazdasági teljesítményt jelent a bányászat, amelynek útján a tulajdonosok minden esetben virtuális elszámolási egységekre tesznek szert. Így a kockázati tényező kizárható, amely szintén alapeleme a büntetendő magatartásnak a Btk. törvényi tényállása szerint. A fentiekben kifejtettek alapján a hálózatot nem lehet olyan piramisrendszernek tekinteni, amelyben a felhasználóktól különböző összegeket csalnak ki annak tervezői.

12. Konklúzió

„A cybertérből szólok hozzátok, fejlett ipari országok kormányai, kik húsból, betonból, acélból építkeztek és merítitek hatalmatokat. A jövő nevében követelem tőletek, kik a múlt-

ból nyeritek erőtöket, hagyjatok minket örökre békén! Nem üdvözlünk benneteket jó szívvel. Ahol mi összegyűlünk, ott nektek semmi erőtök sincsen! Nekünk nincsen választott kormányunk, és soha nem is lesz. Pontosan akkora hatalommal jelentem ki ezt, amennyi magából a szabadság tényéből fakad. Ezennel megalapítom a globális szociális teret, mely eredendően független a zsarnokságotoktól, amit ránk akartok kényszeríteni. Nincsen jogotok az emberi lélek új otthonát szabályozni, és eszközeitek sincsenek arra, hogy a módszereiteknek – melyektől félnünk kellene – érvényt szerezzetek."[85]

A *Cybertér Függetlenségi Nyilatkozatát* John Perry Barlow fogalmazta meg 1996. február 8-án, amelynek kezdő sorai akarva akaratlanul is visszaköszönnek minden egyes alkalommal, amikor az internet szabályozhatósága van terítéken. A technikai fejlődéssel a világháló mindig túlterjeszkedik a törvényeken, ezért lehetetlen hatékonyan és minden részletre kiterjedően szabályozni, mivel mindig lesznek kiskapuk és lefedetlen területek. A nyilatkozat ezt egyszerűen úgy fogalmazza meg, hogy a kormányzatoknak nincs hatalmuk az emberi tevékenység e szintje felett. Jó példa erre a Bitcoin-jelenség is, amely teljesen újszerű megoldásai miatt olyan kérdéseket vet fel, amikre eddig nem volt példa.

A virtuális érme mögött álló technológia olyan újdonság, amely mindeddig példátlan paradigmaváltást jelent a pénzügyi rendszerek terén, és ezért nem is látható teljesen tisztán, hogy mi minden következhet még belőle, hiszen a teljes kibontakoztatásához szükséges eszközök jelenleg is fejlesztés alatt állnak.

Létezik olyan szemlélet is, amely szerint nem is érdemes a Bitcoinra, mint pénzre tekinteni, hanem úgy kell felfogni, mint egy protokollt, amellyel azonnal pénzt küldhetünk a világhálón keresztül bárkinek. Teljesen mindegy, hogy mennyit ér egy Bitérme, mivel előbb-utóbb úgyis átváltjuk más valutára, vagy éppen elköltjük különböző fogyasztási cikkekre.[86]

Ez is jól példázza, hogy jelenleg nagyon nehéz stabil álláspontot kialakítani erről a virtuális jelenségről, hiszen túl új ahhoz, hogy egyértelműen értékelni tudjuk. A Bitcoint először meg kell érteniük és teljes egészében fel kell fogniuk a piaci szereplőknek, így egy idő után ki fog alakulni a megfelelő szemlélet, és ez maga után vonhatja majd az új fizetőeszköz kibontakozását és széleskörű elterjedését is. Optimális szabályozást pedig addig nem lehet hatékonyan kialakítani. Addig is érdemes a Bitcoinra úgy tekinteni, mint pénzre – hiszen e célból tervezték – és így értékelni a piacon és a joggyakorlatban.

Jegyzetek

[1] A tanulmány alapjául a szerző az Infokommunikáció és jog folyóirat 49. számában megjelent cikke szolgál

[2] http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis [2011.10.16.]

[3] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf

[4] http://www.wired.com/magazine/2011/11/mf_bitcoin/ [2012.06.17]

[5] A pénz hagyományos értelemben vett funkciói: csereeszköz funkció, fizetési eszköz funkció, értékmegőrző funkció, elszámolási funkció.

[6] http://infoter.blog.hu/2012/06/11/bitcoin_a_nonkomformista_digitalis_fizetoeszkoz [2012.08.01.]

[7] A cyberpunk a kortárs tömegkultúra egyik népszerű stílusa, lényegében a közeli jövőben játszódó sci-fik altípusa. A cyberpunk művekben az emberek általában óriási, túlzsúfolt metropoliszokban élnek, érzelmi életük ennek megfelelően sivár. A nemzeti érzés helyett a cégekhez tartozás kerül előtérbe. Tipikus szereplők a számítógépes bűnöző és az informatikus szakember.

[8] Ludlow, Peter (szerk.): Crypto Anarchy, Cyberstates, and Pirate Utopias, 2001. ISBN 0-262-62151-7

[9] http://trumpf-3.rz.uni-mannheim.de/www/sem96s/webrum.uni-mannheim.de/bwl/zenner/seminar/ecash.htm [2012.08.01.]

[10] http://www.weidai.com/bmoney.txt [2012.08.01.]

[11] http://unenumerated.blogspot.hu/2005/12/bit-gold.html [2012.08.01.]

[12] http://infoter.blog.hu/2012/06/11/bitcoin_a_nonkomformista_digitalis_fizetoeszkoz [2012.08.01.]

[13] http://hu.wikipedia.org/wiki/Bitcoin [2011.10.26.]

[14] http://bitcoin.org/ [2011.10.16.]

[15] https://en.bitcoin.it/wiki/Wallet [2011.10.26.]

[16] https://en.bitcoin.it/wiki/Securing_your_wallet [2011.10.18.]

[17] http://www.techworld.com.au/article/380396/google_releases_open_source_bitcoin_client/ [2011.10.26.]

[18] http://bitcoins.hu/bitcoin_faq.htm [2011.10.26.]

[19] http://www.economist.com/blogs/babbage/2011/06/virtual-currency [2011.10.17.]

[20] http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.26.]

[21] https://en.bitcoin.it/wiki/Introduction#Transferring_a_coin [2011.10.17.]

[22] Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf [2011.10.17.]

[23] Nakamoto, Satoshi: i.m.

[24] http://wiki.prog.hu/wiki/Hash [2011.10.26.]

[25] http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.26.]

[26] http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.26.]

[27] http://www.origo.hu/techbazis/internet/20110615-bitcoin-a-torrentrol-mintaztak-az-internetes-penzt.html [2011.10.18.]

[28] https://en.bitcoin.it/wiki/Blocks [2011.10.17.]

[29] http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.17.]

[30] http://bitcoin.hu/?page_id=316 [2011.10.27.]

[31] http://bitcoins.hu/index.html [2011.10.16.]

[32] http://www.weusecoins.com/mining-guide.php [2011.10.26.]

[33] https://en.bitcoin.it/wiki/Block [2011.10.16.]

[34] https://en.bitcoin.it/wiki/Introduction#Creation_of_coins [2011.10.16.]

[35] https://en.bitcoin.it/wiki/File:Total_bitcoins_over_time_graph.png [2011.10.26.]

[36] Grinberg, Reuben: Bitcoin: An Innovative Alternative Digital Currency (2011.04.21.). http://ssrn.com/abstract=1817857 [2011.10.19.]

[37] http://bitcoin.hu/?p=74 [2011.10.26.]

[38] http://www.dailytech.com/Inside+the+MegaHack-+of+Bitcoin+the+Full+Story/article21942.htm [2011.10.26.]

[39] http://btc.exchangerates24.com/huf/history/?q=30 [2011.10.26.]

[40] https://en.bitcoin.it/wiki/Trade#Legal_Services [2011.10.18.]

[41] http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable [2011.10.18.]

[42] https://www.torproject.org/ [2011.10.18.]

[43] http://www.zeit.de/2011/27/Internet-Bitcoins [2011.10.19.]

[44] Grinberg, Reuben: i.m.

[45] http://bitcoin.hu/?p=1007 [2011.10.20.]

[46] A Second Life egy interaktív virtuális világ, amely 2003 júniusa óta játszható az Interneten keresztül. Fejlesztő: Linden Lab. Honlap: http://secondlife.com/ [2012.07.31]

[47] http://www.facebook.com/FarmVille [2011.10.20.]

[48] A Diablo III egy internetes „hack and slash" stílusú szerepjáték, amely 2012 májusa óta játszható. Fejlesztő: Blizzard Entertainment. Honlap: http://eu.battle.net/d3/en/?- [2012.07.31]

[49] http://diablo3.hu/2011/08/02/tisztazzuk-a-hallottakat-real-money-auction-house/ [2011.10.20.]

[50] http://tech.fortune.cnn.com/2011/06/17/the-clock-is-ticking-on-bitcoin/ [2011.10.20.]

[51] http://hu.wikipedia.org/wiki/Iraki_din%C3%A1r [2011.10.26.]

[52] Grinberg, Reuben: i.m.

[53] http://hu.wikipedia.org/wiki/P%C3%A9nz#Mag.C3.A1np.C3.A9nz [2011.10.24.]

[54] 2001. évi LVIII. törvény a Magyar Nemzeti Bankról 4.§ (2)

[55] http://en.wikipedia.org/wiki/Liberty_Dollar [2011.10.26.]

[56] http://www.citizen-times.com/article/20110319/NEWS01/110319006/Liberty-Dollar-creator-convicted-federal-court [2011.10.26.]

[57] http://online.wsj.com/article/SB10001424052748704425804576220383673608952.html?mod=googlenews_wsj [2011.10.24.]

[58] 1959. évi IV. törvény a Polgári Törvénykönyvről (Ptk.) 338/A.§ (2)

[59] 2006. évi IV. törvény a gazdasági társaságokról (Gt.) 177.§

[60] Gt. 171.§ (1)

[61] Ptk. 338/A.§ (1)

[62] Lábady, Tamás: A magyar magánjog (polgári jog) általános része. Dialóg Campus Kiadó, Budapest-Pécs 2002. p. 291-292.

[63] 1999. évi LXXVI. törvény a szerző jogról 1.§ (6)

[64] Ptk. 94.§ (1)-(2)

[65] Federal Bureau of Investigation, Intelligence Assasment: Bitoin Virtual Currency: Unique Features Present Distinct Challanges for Deterring Illicit Activity (24. April 2012) Online: http://cryptome.org/2012/05/fbi-bitcoin.pdf [2012.07.31]

[66] Nakamoto Satoshi: i.m.

[67] Federal Bureau of Investigation, Intelligence Assasment: im.

[68] Federal Bureau of Investigation, Intelligence Assasment: im.

[69] A társaság adatai a Tokiói Kereskedelmi és Ipar kamara honlapján: http://www.tokyo-cci.or.jp/english/ibo/2353440.htm [2012.07.31]

[70] https://en.bitcoin.it/wiki/Bitcoin_Laundry [2012.07.31]

[71] Ptk. 94. § (2) bekezdése

[72] http://www.symantec.com/security_response/writeup.jsp?docid=2011-061615-3651-99 [2012.07.08]

[73] Federal Bureau of Investigation, Intelligence Assasment: i.m.

[74] http://hu.spam.wikia.com/wiki/Botnet [2012.07.31]

[75] http://blog.sparktrust.com/?p=572 [2012.07.10]

[76] https://bitcointalk.org/index.php?topic=11506.0 [2012.07.10]

[77] Az Európai Bizottság C7-0293/10 számú javaslata az információs rendszerek elleni támadásokról szóló Európai Parlamenti és Tanácsi 2005/222/IB számú kerethatározat hatályon kívül helyezéséről. Online: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/com/com_com%282010%290517_/com_com%282010%290517_hu.pdf [2012.07.10]

[78] http://thenextweb.com/insider/2011/06/24/lulzsec-claims-to-have-received-over-18000-worth-of-donations/ [2012.07.10]

[79] http://www.hightechforum.org/bitcoins-a-crypto-geek-ponzi-scheme/ [2012.07.30]

[80] Szántó, Judit: Piramisjáték vagy Multi Level Marketing? Szakdolgozat, 2007. Online: http://www.jogiforum.hu/files/publikaciok/szanto_judit-piramisjatek%5Bjogi_forum%5D.pdf [2012.07.30]

[81] A Büntető Törvénykönyvről szóló 1978. évi IV. törvény 299/C. §

[82] https://en.bitcoin.it/wiki/Mining#Difficulty [2012.07.30]

[83] http://bitcoin.hu/?p=2250 [2012.07.30]

[84] https://en.bitcoin.it/wiki/Myths#It.27s_a_giant_ponzi_scheme [2012.07.30]

[85] https://projects.eff.org/~barlow/Declaration-Final.html [2011.10.26.]

[86] http://bitcoin.hu/?p=1280 [2011.10.26.]