

Eszteri Dániel

Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze?

1. Bevezetés

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 büntetendők a jog szerint. Mi a helyzet azonban akkor, ha kitalálunk egy újfajta pénzt? Nos, egy SATOSHI NAKAMOTO nevű japán programozó pont ezt tette 2009 januárjában. Megalkotta a Bitcoin nevű virtuális fizetőeszközt, melyet magyarul Bitérmének fordíthatunk. 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.¹

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

2. Laptopból pénztárca

A Bitcoin (általános rövidítése: BTC) nem kézzelfogható, fizikailag létező fizetőeszköz, hanem virtuális pénz: egy összeg, amely társítva van egy virtuális pénztárcával.² Hogyan is juthatunk hozzá egy ilyen pénztárcához? Először is le kell töltenünk egy ingyenes szoftvert az internetről, melyet - meglepő módon – szintén Bitcoinnak hívnak. A programot a virtuális fizetőeszköz hivatalos honlapján találhatjuk meg.³

Ez a program egyfajta virtuális pénztárcaként funkcionál a számítógépünkön, mely digitális pénzünket tárolja. A pénztárcánk nem más, mint egy fájl a számítógépen, melyet „*wallet.dat*” néven találhatunk meg.⁴ 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 netes szolgáltatások, ahová regisztrálva feltölthetjük a tárcánkat és ahhoz csak megadott jelszavunkkal férhetünk hozzá.⁵ A program nyílt forráskódú, mely minden jelentősebb operációs rendszerre lefordított változatban elérhető, folyamatosan fejlesztik, és a Bitcoinok küldéséhez és fogadásához szükséges minden funkciót tartalmaz.⁶

Miután számítógépünkre sikeresen telepítettük a fenti szoftvert, nincs is más hátra, mint hogy elindítsuk, és akár kezdődhet is a virtuális kereskedelem. 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, melyeket szintén ezzel a szoftverrel készíthetünk magunknak.

Minden egyes felhasználó rendelkezik legalább egy ilyen Bitcoin-címmel, mely logikailag egy e-mail címhez hasonlatos. Különbség a kettő között, hogy ezzel nem szöveges üzeneteket és fájlokat, hanem virtuális pénzt küldhetünk és fogadhatunk.

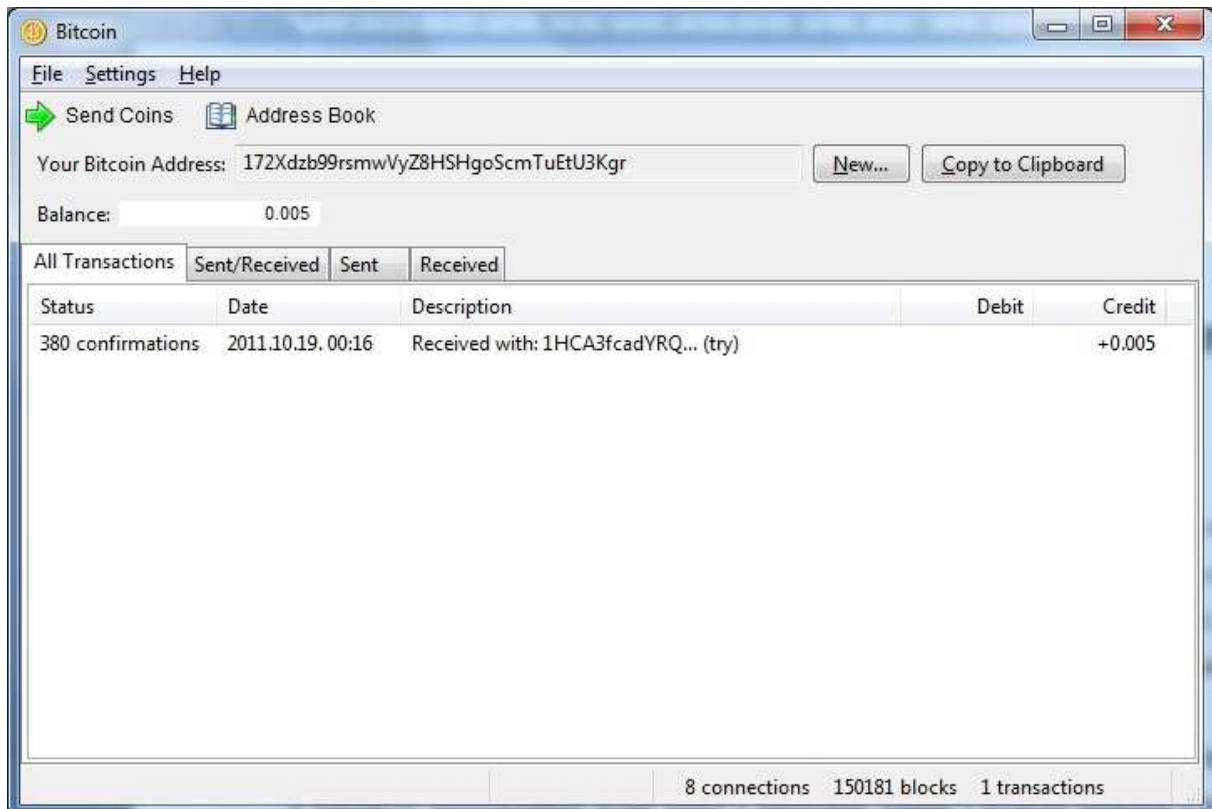
A Bitcoin-címünket a virtuális pénztárca-szoftver kérésünkre automatikusan generálja. A program elméletileg minden egyes tranzakciónkhoz külön címet készít, növelve ezzel az anonimitást, és a rendszer biztonságát. Persze ha megadjuk valamilyen nyilvános fórumon egyik címünket, akkor ezt több átutalásra 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 pénztárcaunkban 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.⁷

A tranzakciók hitelesítéséhez azonban a program nem a nyilvános-, hanem a „*privát kulcsot*” használja, mely 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 érmeinket akkor ne is adjuk meg őket senkinek. Ellentétben a publikus kulcs megadása minden esetben szükséges a tranzakcióhoz.⁸ Hogyan is történnek a tranzakciók, és mi a funkciójuk a címekhez rendelt nyilvános- és privát kulcsoknak?

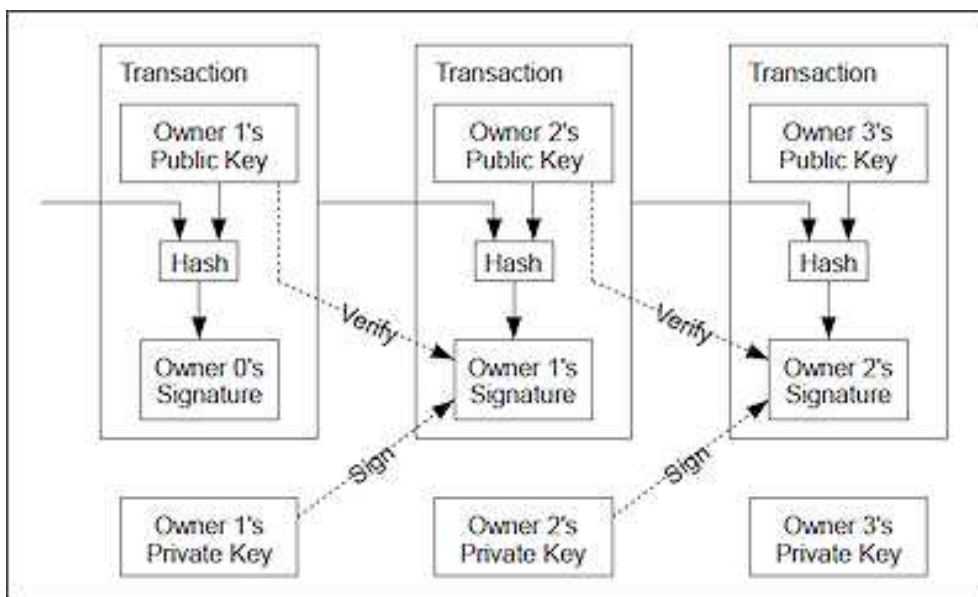
A Bitcoin hálózat a rajta keresztül létrejövő tranzakciókat az egész hálózaton szétküldi, így azok teljesen nyilvánosak. Szemben a hagyományos pénzügyi intézetekkel, amelyek az ügyfelek magánszféráját a tranzakciókra vonatkozó információk visszatartásával védik, ezt a Bitcoin rendszerében az biztosítja, hogy a címek tulajdonosaira vonatkozó információk egyáltalán nem ismertek.⁹ Ha például létrehozok a Bitcoin szoftverrel egy új címet, akkor a program semmilyen információt nem kér tőlem a személyes adataimról. 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 pénztárcaunkba. A rendszer működésére nézzünk egy egyszerű példát.

Tegyük fel, hogy Aliz szeretne küldeni Bencének 10 Bitcoint. Bence ezért megadja Aliznak a virtuális pénztárcajához 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 pénztárcajához, bármelyiket megadhatja, vagy akár készíthet egy újat is csak ehhez az utaláshoz. A pénz végül mindenképpen Bence pénztárcajában 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 „12HnGCwwS4ES1tRC3JXeEYHuFLs9mzMjF7” 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 utalás 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.¹⁰ A tranzakciókat az alábbi ábra szemlélteti.¹¹



3. 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 burkolódhatnak, 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, vagy bármilyen szerv, ami ezt az ellenőrzést végzi. Sok eddigi 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 hasonlók 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.¹² 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 visszafelé az adat, amit titkosított. Viszont a

számot használva ellenőrizhetjük, hogy valóban azzal az adattal van-e dolgunk, amire szükségünk van.¹³

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.¹⁴ 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 le is tölti az összes blokkot a számítógépe merevlemezére (jelenleg kb. 150 ezret, ami hozzávetőlegesen 350 MB), aztán idővel hozzá mindig a legújabbakat. Ilyen redundanciával a világ legbiztonságosabb banki adatbázisa sem rendelkezik.¹⁵ Az összes tranzakció teljes adatbázisa ott van minden egyes ember számítógépén, aki Bitcoint használ és ez 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.¹⁶

Egy idő után ez persze tarthatatlan lesz, mivel a tranzakciók számának növekedésével a blokkok mérete is nőni fog, ezért később lehetőség lesz arra is, hogy a tranzakciónaplónak csak a releváns részeit töltsse le a program.¹⁷ 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 pénzt), ha rendelkezik a csomagban lévő nyilvános kulcsához tartozó privát kulccsal is. A nyilvános és privát kulcspárok a virtuális pénztárcánkban vannak tárolva a számítógépünkön a *wallet.dat* fájlban, éppen ezért a Bitcoin világában ezek a fájlok számítanak a legféltebb kincseknek.¹⁸ Érdemes róluk 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*.¹⁹ 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.

4. Aranybányászat csákány nélkül

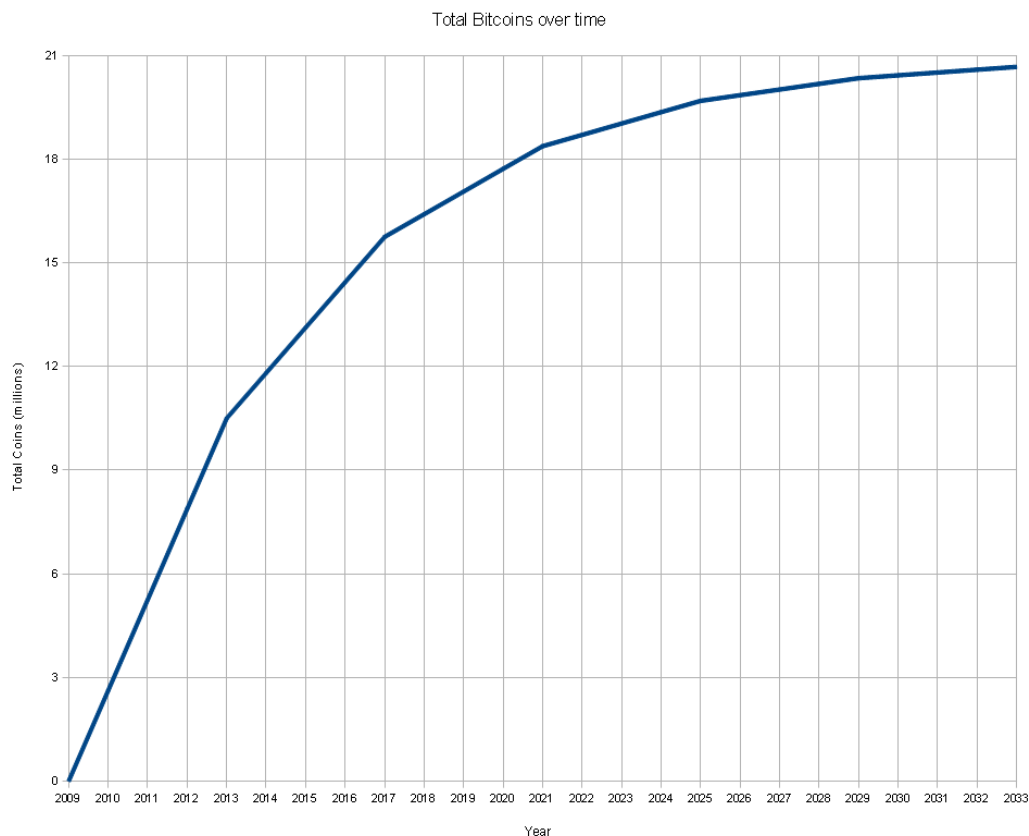
Mivel a Bitcoinoknak nincs központi kibocsátója, ezért felmerül a kérdés, hogy vajon akkor mégis hogyan szerezhetünk belőlük magunknak? Nos, egyrészt vehetjük őket más Bitcoin tulajdonosoktól, vagy nekifoghatunk mi magunk is a termelésének. Mit is kell érteni termelés alatt?

Az új érmék a Bitcoin hálózat csomópontjain generálódnak, amikor a szoftver megoldást talál egy bizonyos matematikai problémára.²⁰ Ahhoz, hogy mi is hozzájárulhassunk a Bitcoinok ilyen úton történő előállításához le kell töltenünk egy szoftvert, amely aztán a számítógépünk processzorának, vagy videokártyájának erőforrásait használja az ilyen matematikai problémák megoldásához eszközül. Az ilyen programokat „*bányász-szoftvernek*” („*mining-software*”) nevezzük, mely a fentebb említett virtuális pénztárca szoftvertől teljesen független program.²¹ Ha sikerült megoldatni a számítógépünkkel a Bitcoin-hálózaton egy matematikai algoritmust, akkor létrejön egy úgy nevezett blokk, melyekben a bitérmék tárolódnak és ezen kívül tartalmazza a velük végzett tranzakciós adatokat is, mint ahogy arról már fentebb szó volt.²² 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.

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 blokkalátalatoknál a jutalmul kapott érmék száma a blokkok aktuális számától is függ. Egy blokk 50 Bitcoinot ér az első 210.000 blokkalátalat esetében. Jelenleg 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 Bitcoinot 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 „kibányásznunk” 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 blokk lesz, amely körülbelül a 2140.-ik évben fog generálódni. Ezután az összes forgalomban lévő érme száma statikus marad, és összesen 20.999.999,- lesz az elérhető érmék száma a világon.²³ Ezt a fajta folyamatot az alábbi ábra szemlélteti.²⁴



5. Mennyit ér egy Bitcoin?

A pénzünket, legyen szó amerikai dollárról, euróról, vagy akár magyar forintról néhány erre specializálódott devizatőzsde honlapon lehet 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.²⁵

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.

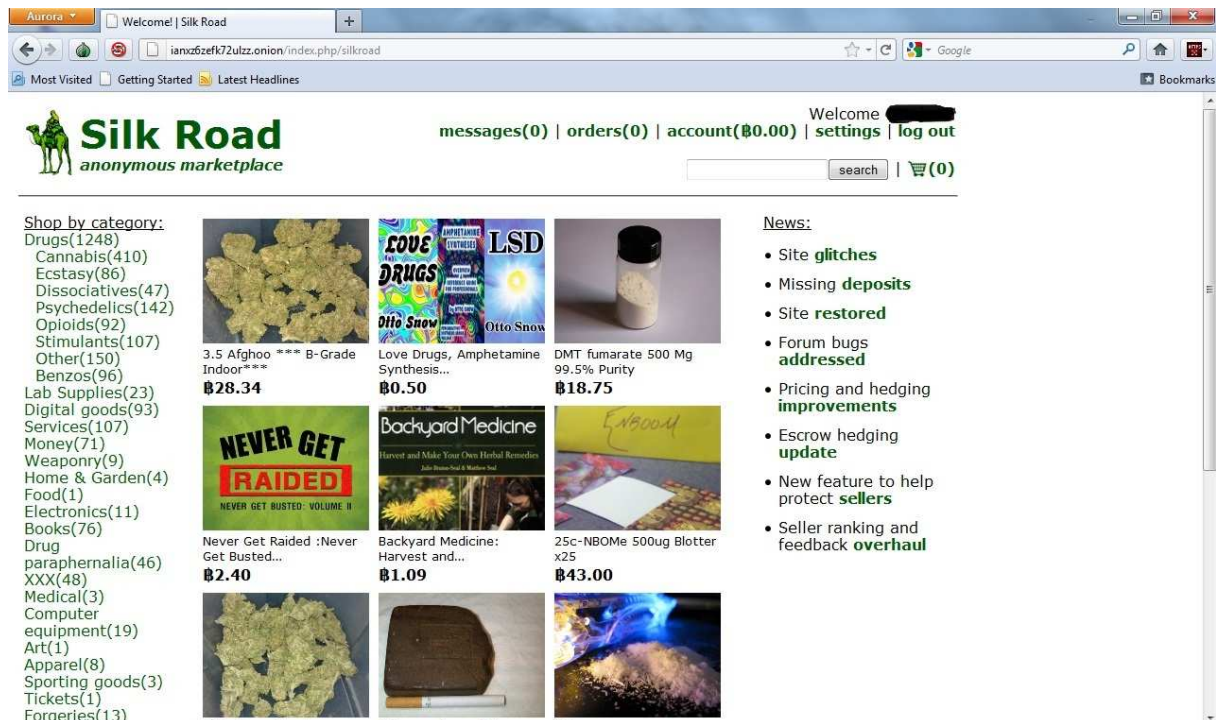
Arra a kérdésre, hogy mégis mennyit ér egy virtuális érme nehéz konkrét választ adni a folyamatos, és olykor igen drasztikus árfolyam ingadozások miatt. Megalkotásakor 2009-ben egy darab érme alig ért többet pár centnél. Ekkor még könnyű volt Bitcoinokhoz jutni, akár egy középkeletű otthoni számítógéppel is tudtunk magunknak bányászni több száz érmét. Miután azonban az emberek elkezdtek 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.²⁶ 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 ez után meredek zuhanásba kezdett, ami még a mai napig is tart.²⁷ A tanulmány írásakor (2011. október vége) egy Bitcoin már „csak” 2,7 dollárt ér, azonban úgy néz ki az árfolyam stabilizálódására számíthatunk a jövőben.²⁸ A Bitcoin egyelőre rendkívül új jelenségnek számít az interneten, így nehéz bármit is jóslni a jövőjét illetően, mivel nem alakultak még ki stabil viselkedési minták vele kapcsolatban.

6. A bizsuktól a kemény drogokig

Tudjuk már, hogyan működik a rendszer és azt is, hogyan juthatunk hozzá ehhez az új fizetőeszközhöz, na de mégis miket vehetünk rajta magunknak? Az interneten számos honlap található, melyen valódi árukért, fogyasztási cikkekért vagy éppen 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.²⁹ Ezek ártatlan és teljesen hétköznapi dolgok, viszont a Bitcoinos pénztátalás 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.³⁰ A weblapot *SilkRoad*-nak hívják és csak egy különleges anonim böngészőt, a *Tor*-t használva tudjuk elérni azt.³¹ Némi keresgélés és regisztráció után, azonban elének tárul a világ legnagyobb drogpiaca, ahol a marihuánától, a heroinon keresztül az LSD-ig mindent meg tudunk rendelni. A drog azonban nem minden: találhatunk itt a természetességhez és előállításához szükséges eszközöket is, de rendelhetünk lőszert, szoftverlicencket, hozzáférési kódokat különböző zárt

weboldalához, robbanóanyagokat és egyéb illegális, vagy épp nehezen beszerezhető termékeket. Fizetni csak és kizárólag egyetlen eszközzel lehet: Bitcoinnal.³²



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 valahogy az alvilágban.

7. Az új fizetőeszköz versenytársairól

A Bitcoinnak legalább három versenytársa van a piacon. Az első csoportba a hagyományos internetes fizetőeszközök tartoznak, amelyek a netes kereskedelmet könnyítik meg, a másodikba 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. Majdnem ugyanolyan, mint a Bitcoin, 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.³³

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 Bitcoin használva ki lehetne küszöbölni.³⁴

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 virtuális tárgyakat. Vannak egyes virtuális világok, ahol játékon belüli pénzünket, akár igazira is átválthatjuk, mint pl. a *Second Life*-ban³⁵. 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*-ben³⁶ 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* 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.³⁷ 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 jó, 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 macerás lenne az elektronikus fizetés. Ennek ellenére létezik New Yorkban egy gyorsétterem, ahol kísérleti céllal lehet már a virtuális érmével is fizetni.³⁸ 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 határozza, 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.

8. Van-e a Bitcoinnak jövője?

Az országok valutái mögött ott vannak 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 nyilatkozta 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 pénz nem 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.³⁹ Irak 2003-as amerikai megszállása után az 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.⁴⁰

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 akadály 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 elharapódnak a lopások. A jövőben előfordulhat például, hogy valaki ír egy trójai vírust, mely megkeresi a számítógépen a virtuális pénztárca fájlt, majd az elküldi a vírus írójának. Mivel az anonim tranzakciós rendszer miatt nem lehet követni az utalásokat, egy ilyen lopás akár egy felhasználó teljes Bitcoin vagyonának elvesztésével járhat. Természetesen a vírusprogram írója utáni nyomozás járhat ettől még sikerrel, de az átutalások követhetlensége miatt sokkal nehezebb is lesz az.

Ezen kívül elveszítheti sokak szemében még a Bitcoin az értékét azon tulajdonsága miatt is, hogy csak az interneten létezik. Ha nincs netkapcsolatunk, akkor Bitcoinunk sincs, hiába van ott a virtuális pénztárca a gépünkön, magát a fájlt nem tudjuk pénzzé tenni sehogy, csak a világhálót használva. 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 Bitcoin decentralizált és biztosítatlan volta nem ítéli automatikusan halálra, viszont a felhasználóknak számolniuk kell azzal, hogy ez az új, még fejlődésben lévő fizetőeszköz akár meg is bukhat a jövőben.

9. 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.⁴¹ 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.⁴² A Bitcoinnak azonban a magánpénzekkel ellentétben nincs hivatalos, központi kibocsátója, hanem azt a felhasználók állítják elő a számítógépek segítségével. Bárki, aki bányász-szoftvert futtat, vagy tagja egy bányász-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, melyet 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.⁴³ Többen is használták a Liberty Dollárt, ami egy idő után szemet szűrt az Egyesült Államokban és végül be is tiltották azt, mint megtévesztő fizetőeszközt. A Bitcoinnal ellentétben azonban ez a valuta biztosítva volt arannyal, ezüsttel és már értékes fémekkel, ráadásul papír és érme formában jelent meg a piacon úgy, mint az egyes államok hivatalos valutái.⁴⁴ Az ítélet indoklása szerint a tiltás nem a magánpénzek elleni támadásként értékelendő, hanem a csalás és pénzhamisítás megelőzését kívánja segíteni.⁴⁵

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 terméként 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.⁴⁶ 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.⁴⁷ 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 a részvénytársasággal szemben a részvény névértékének vagy kibocsátási értékének szolgáltatására terjed ki.⁴⁸ 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 pénzüsszeget szolgáltat az értékpapír jogosultjának.⁴⁹ A Bitcoin azonban nem váltható át előre meghatározott pénzüsszegre 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.⁵⁰ 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.⁵¹ 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 mindenkorai használójának 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 hozzáférésehez 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 pénzáttalálás 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 számítógépek számítási képességének felhasználásával egyfajta terméként 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.⁵² 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.

10. Konklúzió

„A cybertérből szólok hozzátok, fejlett ipari országok kormányai, kik húsból, betonból, acélból építkeztek és merítitek hatalmatokat. A jövő nevében követelem tőletek, kik a múltból nyeritek erőtöket, hagyjatok minket örökre békén! Nem üdvözlünk benneteket jó szívrrel. Ahol mi összegyűlünk, ott nektek semmi erőtok 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 szerezzenek.”⁵³

A *Cybertér Függetlenségi Nyilatkozatát* JOHN PERRY BARLOW fogalmazta meg 1996. február 8.-án melynek kezdő sorai akarva akaratlanul is visszaköszönnék 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, melyekre 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 BTC, mivel előbb-utóbb úgyis átváltjuk más valutára, vagy éppen elköltjük különböző fogyasztási cikkekre.⁵⁴

Ez is jól példázza, hogy jelenleg nagyon nehéz stabil álláspontot kialakítani erről a virtuális jelenségről, hiszen túl új ahhoz, hogy egyértelműen értékelni tudjuk. A Bitcoin 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.

¹ http://www.newyorker.com/reporting/2011/10/10/111010fa_fact_davis [2011.10.16.]

² <http://hu.wikipedia.org/wiki/Bitcoin> [2011.10.26.]

³ <http://bitcoin.org/> [2011.10.16.]

⁴ <https://en.bitcoin.it/wiki/Wallet> [2011.10.26.]

⁵ https://en.bitcoin.it/wiki/Securing_your_wallet [2011.10.18.]

⁶ http://www.techworld.com.au/article/380396/google_releases_open_source_bitcoin_client/ [2011.10.26.]

⁷ http://bitcoins.hu/bitcoin_faq.htm [2011.10.26.]

⁸ <http://www.economist.com/blogs/babbage/2011/06/virtual-currency> [2011.10.17.]

⁹ http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.26.]

¹⁰ https://en.bitcoin.it/wiki/Introduction#Transferring_a_coin [2011.10.17.]

¹¹ Nakamoto, Satoshi: Bitcoin: A Peer-to-Peer Electronic Cash System. <http://bitcoin.org/bitcoin.pdf> [2011.10.17.]

¹² Nakamoto, Satoshi: im.

¹³ <http://wiki.prog.hu/wiki/Hash> [2011.10.26.]

¹⁴ http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.26.]

¹⁵ http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.26.]

¹⁶ <http://www.origo.hu/techbazis/internet/20110615-bitcoin-a-torrentrol-mintaztak-az-internetes-penzet.html> [2011.10.18.]

¹⁷ <https://en.bitcoin.it/wiki/Blocks> [2011.10.17.]

¹⁸ http://bitcoins.hu/bitcoin_geekeknek.htm [2011.10.17.]

¹⁹ http://bitcoin.hu/?page_id=316 [2011.10.27.]

²⁰ <http://bitcoins.hu/index.html> [2011.10.16.]

²¹ <http://www.weusecoins.com/mining-guide.php> [2011.10.26.]

²² <https://en.bitcoin.it/wiki/Block> [2011.10.16.]

²³ https://en.bitcoin.it/wiki/Introduction#Creation_of_coins [2011.10.16.]

²⁴ https://en.bitcoin.it/wiki/File:Total_bitcoins_over_time_graph.png [2011.10.26.]

²⁵ Grinberg, Reuben: Bitcoin: An Innovative Alternative Digital Currency (2011.04.21.). <http://ssrn.com/abstract=1817857> [2011.10.19.]

²⁶ <http://bitcoin.hu/?p=74> [2011.10.26.]

²⁷ <http://www.dailytech.com/Inside+the+MegaHack+of+Bitcoin+the+Full+Story/article21942.htm> [2011.10.26.]

²⁸ <http://btc.exchangerates24.com/huf/history/?q=30> [2011.10.26.]

²⁹ https://en.bitcoin.it/wiki/Trade#Legal_Services [2011.10.18.]

³⁰ <http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable> [2011.10.18.]

³¹ <https://www.torproject.org/> [2011.10.18.]

³² <http://www.zeit.de/2011/27/Internet-Bitcoins> [2011.10.19.]

³³ Grinberg, Reuben: im.

³⁴ <http://bitcoin.hu/?p=1007> [2011.10.20.]

³⁵ <http://secondlife.com/> [2011.10.20.]

³⁶ <http://www.facebook.com/FarmVille> [2011.10.20.]

³⁷ <http://diablo3.hu/2011/08/02/tisztazzuk-a-hallottakat-real-money-auction-house/> [2011.10.20.]

³⁸ <http://tech.fortune.cnn.com/2011/06/17/the-clock-is-ticking-on-bitcoin/> [2011.10.20.]

³⁹ http://hu.wikipedia.org/wiki/Iraki_din%C3%A1r [2011.10.26.]

⁴⁰Grinberg, Reuben: im.

⁴¹<http://hu.wikipedia.org/wiki/P%C3%A9nz#Mag.C3.A1np.C3.A9nz> [2011.10.24.]

⁴²2001. évi LVIII. törvény a Magyar Nemzeti Bankról 4.§ (2)

⁴³http://en.wikipedia.org/wiki/Liberty_Dollar [2011.10.26.]

⁴⁴<http://www.citizen-times.com/article/20110319/NEWS01/110319006/Liberty-Dollar-creator-convicted-federal-court> [2011.10.26.]

⁴⁵http://online.wsj.com/article/SB10001424052748704425804576220383673608952.html?mod=googlenews_ws
j [2011.10.24.]

⁴⁶1959. évi IV. törvény a Polgári Törvénykönyvről (Ptk.) 338/A.§ (2)

⁴⁷2006. évi IV. törvény a gazdasági társaságokról (Gt.) 177.§

⁴⁸Gt. 171.§ (1)

⁴⁹Ptk. 338/A.§ (1)

⁵⁰Lábady, Tamás: A magyar magánjog (polgári jog) általános része. Dialóg Campus Kiadó, 2002. p. 291-292.

⁵¹1999. évi LXXVI. törvény a szerző jogról 1.§ (6)

⁵²Ptk. 94.§ (1)-(2)

⁵³<https://projects.eff.org/~barlow/Declaration-Final.html> [2011.10.26.]

⁵⁴<http://bitcoin.hu/?p=1280> [2011.10.26.]