

NEMZETBIZTONSÁGI SZEMLE

MMXIV.

II. ÉVFOLYAM II. SZÁM

KÜLÖNLENYOMAT



NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI INTÉZET
BUDAPEST

Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei

Gazdag Tibor – Kovács Zoltán³⁴

Absztrakt

A kommunikáció mellett más internet alapú szolgáltatások ellenőrzése is fontos az arra feljogosított szervezetek számára. Ilyenek például a banki szolgáltatások. Ahogyan a hagyományos hírközlést alapjaiban változtatja/változtatta meg az internet, úgy ez – ha jelenleg ugyan még csak csekélyebb mértékben, de – elmondható a pénzügyi szektorról is. A hagyományos pénzügyi tranzakciókat interneten keresztül biztosító banki megoldások mellett sorra jelennek meg az alternatív lehetőségek. Ezek közül vannak, amelyek kifejezetten virtuális pénzt kibocsátva nyújtanak pénzügyi szolgáltatásokat, sőt adott esetben teljesen legális, hagyományos web-boltban (pl. Wordpress store) is lehet fizetni velük (pl. Bitcoin), és vannak, amelyek csupán „melléktermékként”, de hasonló virtuális pénzműveletekre adnak lehetőséget (pl. Diablo III). Az új, alternatív pénzügyi tranzakciós lehetőségek kényelmet és egyszerűséget biztosítanak a felhasználók számára, azonban számos veszélyt is magukban hordoznak. A cikk néhány új tranzakciós lehetőség ismertetésén keresztül bemutatja azok veszélyeit és a törvényes ellenőrzés során megjelenő nehézségeket is.

Kulcsszavak: felhő alapú rendszerek, BitCoin, törvényes ellenőrzés,

New financial transaction possibilities by cloud computing systems and their dangers

Abstract

Besides the lawful monitoring of communication based on Internet, there are some other application services, which have to be monitored by national security services and law enforcement agencies. These are for example banking services. As the classic communication has been fundamentally changed by Internet, this can be said (but in a lesser extent) about the financial sector as well. Beside the money transaction solutions via Internet provided by banks, new alternative possibilities are appearing. Some of these are offering financial services by supplying virtual money, moreover in given cases you can pay with it (e.g. Bitcoin) in completely legal web-shops (e.g. Wordpress store), and

³⁴ gazdagtibor@me.com, zkovacs@nbsz.gov.hu

some of them are just by-products, but they give similar possibilities for similar virtual financial operations (e.g. Diablo III). The new alternative financial transactions ensure convenience and simplicity for the users, although they also involve threats. This article presents their threats and the difficulty of lawful monitoring of them through the description of some of these methods.

Key words: cloud computing, BitCoin, lawful monitoring

Bevezetés

Felgyorsult életritmusunk, a – sokszor napi nyolc órát meghaladó – munka melletti számtalan kötelezettség, egyéb teendőink okán egy-egy feladat, ügy elintézésére egyre kevesebb időnk marad. Az internet és az internet-alapú alkalmazások segítenek abban, hogy számtalan teendőnket gyorsabban, kényelemsebben, sorban állás nélkül akár otthonról is elintézhessük.

Ennek igénye megjelenik pénzügyeink rendezésében is. A szélessávú internet és a személyi infokommunikációs eszközök széleskörű elterjedésével a felhasználók pénzügyi tranzakcióikat is szeretnék gyorsan, kényelmesen, egyszerűen elintézni.

A megváltozott igényekre és technikai lehetőségekre a bankok azonban rugalmatlanul reagálnak. Konzervatív működési szemléletük és a biztonság feltétlen megteremtésének szándéka védi ugyan a felhasználókat, ugyanakkor éppen e miatt az újonnan jelentkező igényeket nem, vagy csak hosszú átfutási idő után képesek kielégíteni. A „piaci rést” azonban, mint minden más ágazatban, a vállalkozó szellemű emberek hamar felismerik, és annak betöltésére megoldásokat kezdenek el kínálni. Így megjelennek olyan, korábban nem látott alternatív pénzügyi lehetőségek, mint a virtuális valuta használata.

A kényelemnek, mint mindenhol, természetesen itt is ára van. Az új pénzügyi lehetőségek ugyanis kockázatosabbak, mint a hagyományos bankok által nyújtott szolgáltatások. Egyfelől magasabb a pénzügyi kockázatuk, hiszen például a virtuális valuták árfolyama könnyebben változik, vagy akár dől be, mint a hagyományos valutáké. Másfelől a virtuális fizetési módok új lehetőségeket teremtenek a bűnözők számára is. Támadásaikkal könnyebben szerezhetik meg mások pénzét, de kétes eredetű pénzüket egyszerűbben és „biztonságosabban” képesek tisztára mosni, vagy másoknak, pl. terroristáknak eljuttatni. Éppen ezért célszerű áttekinteni az új pénzügyi tranzakciós lehetőségeket, azok veszélyeit és a törvényes ellenőrzés során megjelenő nehézségeket.

Új pénzügyi tranzakciós lehetőségek a virtuális térben

Napjainkban az internet és az azt használó alkalmazások gyökeresen változtatják meg szokásainkat, teszik kényelmesebbé életünket. Ilyen kényelmi lehetőség az, hogy saját, ma már javarészt hordozható infokommunikációs eszközeinkkel vásároljunk, bankoljunk akár az otthoni karosszékéből, egy kávézóból, vagy ahol, és amikor időnk engedi. [1] [2] A fejlődés markánsan kimutatható a pénzügyi tranzakciók világában is, hiszen a kibertérben a fizetésre, a pénzügyi tranzakciók végrehajtására számos új lehetőség áll rendelkezésünkre. A klasszikus bankok korábbi szolgáltatásaitak virtualizálják, eddig nem látott, már kifejezetten az internet-technológiára épülőket vezetnek be. Mellettük azonban megjelennek olyan alternatív pénzügyi tranzakciós lehetőségek is, amelyek úgy kínálják ezeket a szolgáltatásokat, hogy a mögöttük álló szolgáltató nem rendelkezik klasszikus banki háttérrel (ilyen például a Bitcoin, továbbiakban: BTC). [2] [3] [4] [5]

Ez utóbbiaknak kétségtelenül az előnyei közé sorolható, hogy gyorsak, egyszerűen, bárki által használhatók, és sokszor olyan igényeket is kielégítenek, amelyeket a klasszikus bankok nem tudnak, vagy nem akarnak.

Az alternatív pénzügyi tranzakciós lehetőségeknek azonban árnyoldalai is vannak. Az egyik a pénzügyi kockázat. Az ugyanis, hogy a szolgáltató nem rendelkezik klasszikus banki háttérrel, kockázatosá teszi, teheti az ügyleteket.

Ezek a pénzügyi kockázatok a felhasználó részéről (ki)számíthatók, vagy legalábbis figyelembe vehetők. Nagyobb, de immár az állam számára jelentkező gondot okoz, hogy bizonyos felhő alapú rendszeren folytatott pénzügyi tevékenységgel úgy lehet jövedelemre szert tenni, hogy az akár teljes mértékben kikerülhet az adóhatóság ellenőrzése alól. Ez pedig nyilvánvalóan ugyanolyan problémát jelent, mint bármilyen más eltitkolt, nem adózott jövedelem. Ám a legsúlyosabb következményei mégis annak vannak, hogy ezek a tranzakciók lehetőséget biztosítanak a pénzmosásra – annak új formáit teremtve meg –, így például a szervezett bűnözés vagy a terrorizmus finanszírozására is. [6]

Az előző bekezdésben a felhő alapú rendszerek említése nem volt véletlen. Az alternatív pénzügyi tranzakciókhoz ugyanis alapvetően internet-technológiára épülő szolgáltatásokat, azon belül is elsősorban nyilvános számítási felhő (Public cloud (PC)) és szoftver, mint szolgáltatás (Cloud Software as a Service (SaaS)) típusú rendszereket (továbbiakban: PC/SaaS felhő alapú rendszerek) használunk fel. A PC/SaaS rendszerek azok a mindenki számára – a meglévő személyi használatú eszközök (pl. notebook, okostelefon stb.) felhasználásával, akár csekély számítástechnikai tudással is használható, olcsón, sokszor ingyenesen – igénybe vehető rendszerek, szolgáltatások (mint pl. Facebook, gmail, Dropbox, Twitter,

Skype stb.) amelyek ma már szerves részét képezik mindennapi életünknek, kommunikációnknak. Ezek között pedig már szép számmal vannak olyanok, amelyekkel pénzügyi tranzakciókat is végrehajthatunk (mint pl. Gmail(!)[7] [8], PayPal, Bitcoin stb.) (A PC/SaaS rendszerek az internet-technológiára épülő szolgáltatások részhalmazának tekinthetők, ám a határvonalat, hogy mikor tekinthető csak az egyiknek vagy mindkettőnek egy szolgáltatás, nagyon nehéz egyértelműen meghúzni. A probléma elemzése jelen cikk keretein túlmutat, ezért a továbbiakban mindenhol PC/SaaS rendszereket említünk.)

A célszemélyek pénzügyi tranzakcióinak az ellenőrzése – különböző formában és mélységben – jelenleg is feladata a nemzetbiztonsági szolgálatoknak, a rendvédelmi szerveknek és az adóhatóságnak is. Ennek a feladatnak egy saját országban (is) működő bank esetén viszonylag egyszerűen eleget lehet tenni. A csak külföldön telephellyel rendelkező, de belföldön is szolgáltatást nyújtó bankok viszonylatában azonban már nehézségekbe ütközhet a törvényes ellenőrzés keretében a szükséges adatok beszerzése. Gondoljunk itt például a svájci bankok felhasználóira, akikről hosszú évtizedekig nem voltak hajlandók kiadni a svájciak semmilyen információt, még akkor sem, ha mindenki által elismerten illegális-, vagy bűncselekményből származó értékek kerültek náluk elhelyezésre. [9] [10] [11] Az online, felhő alapú rendszerek esetében a helyzet pedig még rosszabb. Sokszor a pénzügyi tranzakciót lehetővé tévő alkalmazásszolgáltatók saját magukat sem tartják pénzügyi szervezetnek, vagy a pénzügyi világ nem ismeri el őket azoknak [5]. A felhő alapú rendszerekre jellemző, hogy nem csak a pénzügyi, hanem minden más alkalmazásszolgáltatótól is rendkívül nehéz a törvényes ellenőrzés által kért információk beszerzése. [12]

A világ változásait a bankok ha lassan is, de követik. Így az internet és a személyi használatú infokommunikációs eszközök terjedésével az általuk kínált szolgáltatások szolgáltatásokat is sorra elektronizálják és kínálják ilyen formában is ügyfeleiknek. Ma már egyszerűen, gyorsan utalhatunk pénzt egy másik számlára, fizethetünk be csekkeket, vagy éppen fizethetünk web boltokban akár erre dedikált bankkártyával. [13] [14] A bankok által kínált elektronikus pénzügyi tranzakciók többsége a korábbi banki szolgáltatások átkonvertálása a virtuális világba, annak előnyeit azonban csak lassan fedezik fel és építik be szolgáltatásaikba (pl. egy elektronikusan indított átutalással ne kelljen kötelezően megvárni a következő banki napot, hanem az 4 órán belül megtörténjen). [15] Az új lehetőségek bevezetésének lassúságát persze magyarázza a szigorú jogszabályi környezet, a lehetőleg teljes körű biztonságra törekvés, ám éppen ez a lassúság az, amely miatt egyre gyorsuló világunkban a felhasználók alternatív lehetőségek felé fordulnak.

A bankok nem csak lassan reagálnak az új kihívásokra, lehetőségekre, de sokszor nem is kínálnak megfelelő megoldásokat az „online világ” számára. Így sorra jelennek meg a kifejezetten online világra szabott, pénzügyi tranzakciókat biztosító lehetőségek. Ilyenek például a PayPal, amely havidíj nélkül kínálja biztonságos, sőt pénz-visszafizetési garanciával hirdetett szolgáltatását, amellyel sokszor olcsóbban is lehet online vásárolni. [16] Hasonló biztonságos online fizetést kínál a Neteller, [17] a Moneybookers, vagy újabb nevén a Skrill emellett már magán-személyek közötti tranzakciókat is biztosítja. [18]

Jelenleg még extrém, a jövőben talán már köznapi lesz a peer-to-peer (P2P) hitelezés példája, amely a bankoknál alacsonyabb kamattal és nagyobb megtérüléssel kecsegtet a kis-, és középvállalatok számára. Így az ezen vállalatok finanszírozásával az alacsony nyereség miatt kevesebbet törődő bankok helyét egyre inkább P2P finanszírozásra szakosodott vállalatok veszik át. Az üzleti lehetőség komolyságát mutatja, hogy Nagy-Britanniában középtávon 12 milliárd fontos forgalommal számolnak, az Egyesült Államokban pedig mintegy 100 milliárd dollárra becsülik az említett vállalatok kielégíthetetlen finanszírozási igényét. [19]

Mindezek mellett mégis talán a hagyományos pénzügyi struktúrától való elszakadást a Bitcoin és a hozzá hasonló teljesen virtualizált fizető eszközök, rendszerek jelentik. Ezeket nagyjából két csoportra különíthetjük el: az egyikbe a valódi gazdasághoz kapcsolódónak szánt, a valódi fizetőeszközök valamiféle alternatívájának tervezettek (pl. Flattr, Ripple, Ven, Bitcoin stb.) a másikba az internetes játékokból (Second Life/Linden Dollar, World of Warcraft/Gold stb.) kinövők tartoznak. [20]

A virtuális fizetőeszközök napjainkra – úgy tűnik – gombamód szaporodnak, egy cikkíró legalább 83 félért számolt össze belőlük. [21] Ezek közül a Bitcoint érdemes részletesebben is megvizsgálni. Egyrészt azért mert talán ez a legelterjedtebb, legismertebb virtuális fizetőeszköz, másrészt pedig azért, mert – legalábbis a jelenlegi többi hasonló megoldáshoz képest – viszonylag hosszabb életűnek és „életképesebbnek” tűnik (a Bitcoin 2008-ban indult). [22]

BITCOIN bemutatása

A Bitcoin un. ősblokkját 2009. január 3-án hozta létre egy Satoshi Nakamoto néven fórumozó ismeretlen, bár sokkal valószínűbb, hogy a név nem csupán egy embert takar. A BTC nyílt forráskódú digitális valutánem, amely elnevezés egyrészt egy, a virtuális fizetőeszközt kezelő nyílt forráskódú, bárki által fejleszthető szoftverre, másrészt pedig annak közvetítését szolgáló peer-to-peer hálózatra utal. Ez utóbbi talán a legjelentősebb újítás, hiszen az eddigi elektronikus fizető-

eszközökkel szemben a BTC nem igényel külön infrastruktúrát, így nem kell számolni annak költségeivel sem.

Bitcoin-jainkat bármilyen erre alkalmas eszközön (pl. személyi számítógépen, mobiltelefonon, külső adathordozókon, vagy akár felhő alapú szolgáltatóknál) tárolhatjuk, a tranzakciókhoz pedig csak a küldő és a fogadó címe szükséges. A hagyományos banki rendszerrel szemben BTC hálózatában nincs központi irányítás, így ez kizárja a hatósági kontrollt és befolyást (pl. csalás gyanúja miatt nem lehet sztorozni korábban jóváhagyott tranzakciókat), valamint ugyanezért itt kizárt a manipuláció vagy akár az infláció is. [23]

A Bitcoin más módon is védett. Ez ugyanis egy olyan virtuális fizetőeszköz, melyet egy decentralizált, titkosítással védett, elosztott (P2P) hálózat tárol. A titkosítás erősségére jellemző, hogy a fájlok dekódolása jelenlegi ismereteink szerint belátható időn belül nem lehetséges. A hálózathoz csatlakozás abból áll, hogy egy letöltött kliensprogramot futattunk a számítógépünkön, mely telepítés után rögtön generál egy – a rendszert használók számára – nyilvános számlaszámot (kvázi bankszámla), amellyel tranzakciókat indíthatunk és fogadhatunk.

A kliensek letöltésének számát tekintve első az Egyesült Államok, melyet Kína követ, majd Nagy-Britannia, Németország és Oroszország következik. Magyarország - lakosságához viszonyítva - az előkelő 31. helyen áll. [24] A rendszer karbantartását és fejlesztését önkéntesek végzik, az új Bitcoinok generálását és a tranzakciók nyilvántartását, nyomon követését a rendszer biztosítja.

A rendszer mellett a tulajdonos is védett: az adott BTC felett csak a tulajdonos rendelkezhet, és a számlák befagyasztását vagy lefoglalását "a rendszeren kívülieknek" csak a P2P rendszerben lévő összes számítógép egyszerre történő lekapcsolásával lehetne kivitelezni. A tranzakciók blokkokban kerülnek tárolásra, és minden blokk tartalmazza az előzőek egy részét is. Ez az egymásra épülő, kódolt láncolat biztosítja a tranzakciók hamisíthatatlanságát.

Új BTC-k - jelenleg - átlagosan tízpercenként kerülnek be a rendszerbe, ötvenes csomagokban, melyek négyévente feleződnek, így érik el a 2140-ik évben a rendszert megalkotók által maximálisan meghatározott 21 millió darabot. A BTC-nek "váltópénze" nincs, de nyolc tizedes-jegyig oszthatóak (míg a valós fizetőeszközök két tizedesjegyig), a rendszer tehát megfelelően flexibilis. Mivel előre ismert a maximálisan előállítható Bitcoin, és előállításának üteme is kiszámítható és kizárólag a kereslet-kínálat határozza meg a pillanatnyi értékét, ezért - szemben a hagyományos fizetőeszközök számának változásától (jegybankok "bankoprése" vagy pénz-leértékelése) stabilabb és független az ad-hoc hatásoktól. Forgalmának volumene, intenzitása publikus: nemcsak a Bitcoin-tőzsdéken, hanem

más weboldalakon is figyelemmel kísérhető (bitcoinwatch.com, bitcoinmonitor.com).

A Bitcoinhoz hozzájuthatunk elektronikus tevékenységgel (számítási teljesítménnyel), amely részben bányászattal történik: a blokkok hitelesítéséért végzett számításokat végzőt újonnan létrehozott BTC-vel "díjazza" a rendszer, továbbá a tranzakciós kód előállításában való részvételért is kapható "jutalék". Jelenleg még a "bányászat" tekinthető a hozzájutás fő forrásának, de a számítási feladatok növekvő bonyolultsága miatt idővel szinte egyeduralkodóvá fog válni a tranzakciós jutalék.

A „Bitcoin-láz” vonzataként megjelentek a BTC-előállítására specializált célszámítógépek, és már ezek forgalmazásával is lehet napjainkban vagyont keressen. [25]

A BTC megszerzésének másik útja már hagyományos megoldásnak tekinthető: fizikai fizetőeszköz átváltásával valamint áruk és szolgáltatások nyújtásával lehet szert tenni a virtuális fizetőeszközre.

A BTC-tranzakciókat kétarcúság jellemzi: egyszerre gyorsak (nincs banki záróra) egyben relatíve lassúak (a rendszer mintegy tíz perc alatt ellenőrzi a tulajdonos Bitcoinjának tranzakciós előzményeinek valóságát). A pénzügyi mozgások egy nyílt és egy titkos kulcs felhasználásával kerülnek kódolásra, így a teljes rendszer tudomást szerez a tranzakcióról (de a felek kilétéről nem). Minden számítógépen megtalálható - kódolt formában - a teljes, és egyetlen blokkláncolat, tehát egy visszaélési szándékkal ("hamis pénz") generált kódsorozat nem kerülhet be a láncolatba, így ugyanazt a Bitcoint sem tudja a tulajdonosa kétszer elkölteni...

A Bitcoinnak ellenzői szerint nincs tranzakciós, értékmérő vagy megtakarítási szerepe, tehát nem lehet pénzként definiálni. [26] Támogatói ugyanakkor azzal érvelnek, hogy az Európai Központi Bank fenntartja a jogot a Bitcoin-kérdés szabályozására, az Amerikai Egyesült Államok Kincstára szerint pedig pénzközvetítői szerepe van, mely érvek alátámasztják a BTC fizetőeszközkénti létezését. Németországban hivatalosan elismert fizetőeszköz, az USA egyik bírósága pedig egy piramisjáték szervezőjét ítélte el, indoklásában leszögezve, hogy a Bitcoin fizetőeszköz, a Forbes újságírója pedig egy hétig élt kizárólag BTC felhasználásával, a hagyományos fizetési lehetőségeket mellőzve.

Érdekes, hogy az orosz Legfőbb Ügyészség a Bitcoin használatát betiltó érvelelése is elismeri pénzhelyettesítő szerepét: *„Az anonimitást biztosító fizetési rendszerek és digitális valuták – köztük a legismertebb, a Bitcoin – pénzhelyettesítőnek minősülnek, és sem magánszemélyek, sem intézmények nem használhatják őket.”* [27] [28] [29]

A virtuális fizetőeszköz előnyei között sorolható fel, hogy gyakorlatilag anonim, kívülről számára visszakövethetetlen, bárhol tárolható (virtuális "pénztárca" - eWallet, PC, okostelefon, felhő alapú tároló szolgáltatás stb.), könnyen hozzáférhető, biztonságos (a saját pénzként használható kódsorozat több példányban is tárolható). Előny és hátrány is lehet, hogy a rendszerben nincs "feketelista" sem, nem akadályozható meg az egyes számlákra, vagy azokról indított utalás, sem zárolni, sem lefoglalni nem lehet azokat, amely jellemzők miatt a köztörvényes és a politikai indíttatású bűnelkövetők, vagy akár például terrorizmust támogatók körében is preferált lehet. A BTC-szisztéma hátrányaként róható fel, hogy a legkisebb értékű tranzakció is hosszú időt vesz igénybe, és az egyes államok szabályozásukkal is ellehetetleníthetik (pl. Thaiföld után Kína és Oroszország is betiltotta a használatát.) [29] [30] [31]

A BTC felhasználásánál két fő területet határozhatunk meg: míg egyfelől a hagyományos fizetőeszközök kiváltására, helyettesítésére is alkalmas, mások kifejezetten befektetési céllal szerzik be. Egyes pénzügyi befektetők már megalapították Bitcoin befektetési alapjukat is. A kínaiak úgy tekintenek a Bitcoinra, mint egy kiváló digitális értékfordozóra, valamiféle digitális aranyra. [32] [33] Napjainkban már a legkülönbözőbb adásvételek és szolgáltatások fizetőeszközüvé vált, a pizzától egészen az aranyig, vagy webhosting-díjtól a lakbérfizetésen keresztül a mesterséges megtermékenyítésig. [34] [35] Sőt az első Bitcoin automaták is megjelentek a piacon [36] A jogellenes tevékenységet lehetővé tevő szerepét tekintve mindkét terület érdekes az állam, az adó- és pénzügyi rendszer és a rendvédelem-hírszerzés szempontjából is.

A BTC első látásra teljesen virtualizált és anonimizált fizetőeszköz, amelyben a Bitcoint birtokoló tulajdonosok kiléte nem ismert. A BTC használatakor csupán „account”-jkkal azonosítják magukat, személyazonosságukat csak a hagyományos pénzügyi-gazdasági felülethez történő kapcsolódás során, néhány speciális tranzakciótípus (valuta-BTC átváltása, áru- vagy szolgáltatás vásárlása esetén) fedik fel. Ezek a tulajdonságok azonban nemcsak biztonságot nyújtanak, de nagyfokú kockázatot is rejtenek tulajdonosaik számára.



7. ábra. Bitcoin árfolyamváltozása 2013-ban és 2014 elején³⁵

A „hagyományos” valuták esetén a rendszer kiterjedtsége, a fizetőeszközök kibocsátó államok, a pénzügyi szervezetek, cégek és a gazdasági szereplők száma, rétegzettség és mérete a gyors változások ellen – pusztán tömegük következtében – nagyfokú rezisztenciára és kompenzációra képes. A viszonylag kicsi Bitcoin-piac kevésbé tud ellenállni a negatív vagy pozitív hírek okozta változásoknak, így vagyonok keletkezhetnek vagy tűnhetnek el napok leforgása alatt.

2013 tavaszán a BTC árfolyama 14 USA dollárról (továbbiakban: USD) 238-ra ugrott fel, majd hirtelen a kevesebb, mint a felére, 84-re esett vissza. Október közepétől az árfolyam meredek emelkedésbe kezdett és kisebb zökkenőkkel eljutott – az eddigi – 1 203 USD-s rekordárig, majd 584-re esett vissza. Ez a rendkívül gyors árfolyamváltozás a „hagyományos” valuták esetén nem jellemző, csupán a gazdaságilag instabil országok esetében fordul elő. [37] [38]

A dolog persze érthető, hiszen a hagyományos pénzügyi rendszer stabilitását – főleg a tőzsdei- és hitelügyletek kiterjedésével és a papírpénz mögötti nemesfém fedezet megszűnésével – a szerződések betartásába (betarthatóságába), a pénzügyi rendszer, az árucikkek és szolgáltatások viszonylagos értékállóságába vetett hit tartja fenn. Ez azonban a Bitcoin esetében, egy teljesen anonimizált és

³⁵ Forrás: [http://blockchain.info/hu/charts/market-price?timespan=1year&showDatapoints=false&daysAverageString=1&show_header=true&scale=0&address=\(letöltve: 2014. 03. 02.\)](http://blockchain.info/hu/charts/market-price?timespan=1year&showDatapoints=false&daysAverageString=1&show_header=true&scale=0&address=(letöltve: 2014. 03. 02.))

virtuális környezetben, – jelenleg még legalábbis – nehezen tartható meg hosszabb távon.

Egyes számítások szerint a feketegazdaság világméretű forgalma elérheti a 4000 milliárd dollárt, melybe beleértendő a csempészett doboz cigarettától kezdve a fegyver-feketekereskedelem is. Ebből a pénzforgalomból részesedhet a kalkuláció szerint a Bitcoin is, mintegy 60 milliárd értékben. [39] (A BTC tőzsdei kapitalizációját jelenleg mintegy 3,8 milliárd dollár értékre becsülik.) A jelzett mennyiségű “piszkos pénz” önmagában is a BTC árfolyamának megtöbbszöröződését indukálhatja.

A jogellenes tevékenységből származó pénzek elsősorban az alábbi területről jelenhetnek meg a virtuális pénz világában:

- a “hagyományos” tevékenységek közül:
 - illegális kereskedelem (gyermekpornó, emberkereskedelem, kábítószer, gyógyszer, fegyver),
 - adócsalás, pénzmosás (az egyre inkább visszaszorított off-shore technikákkal szemben),
 - illegális szerencsejáték,
 - illegális kampányfinanszírozás,
 - terrorizmus finanszírozása.
- IT-környezetben
 - a számítógépes - úgynevezett - “0. napi” sérülékenységek,
 - botnet-bérlések (pl. DDoS támadások céljából), [40]
 - erőforrás-lopás (a botnetek már nemcsak spamelésre vagy túlterheléses támadásokra vehetők igénybe, hanem BTC-bányászatra is). [41]
- a Bitcoin-környezet támadására
 - adatlopás (e-pénztárca) [42]
 - account-lopás (pl. Scribd online könyvtárszolgáltató sérelmére) [43]
 - virtuális bankrablás (pl. BitFloor valutaváltó sérelmére) [44]
 - túlterheléses támadással a Bitcoin-tőzsde üzleteinek akadályozására (árfolyam-manipuláció) [45] [46]

A Bitcoin-“iparág” napjainkra már kialakította a virtuális pénz tulajdonosainak és tranzakcióinak anonimitását, visszakövethetlenségét lehetővé tevő megoldásainak széles spektrumát, az IT-területen korábban is alkalmazott általános megoldásoktól a teljesen új, csak itt alkalmazható megoldásokig. Egyes felhasználók internetes identitását, forgalmazását anonimizáló proxy szerverek “védik”, akár tranzakciónként is új BTC azonosítót generálhatnak, külső e-tárca szolgáltatót vesznek igénybe, névtelenítő átváltási technikát (BTC-ZeroCoin-BTC) vezettek be illetve specializálódott “virtuális pénzmossó” cégeken folytatják keresztül pénzeiket. (A cég - jutalék fejében - több accountról aggregálja egybe a virtuális pénzt, illetve több számlára osztja szét, vagy az egyes tulajdonosok Bitcoinjait utalja körbe, keveri össze.) [47] [48] [49]

Egyes kutatók azonban figyelmeztetnek, hogy teljes anonimitás nem létezik a BTC világában sem. [50] Amennyiben nem vesznek igénybe anonimizáló technológiát, a felhasználók IP-címe nyilvános és megismerhető, akik egyébként is gyakran óvatlanok, mikor internetes fórumokon közzéteszik accountjuk adatait. Minden egyes korábbi forgalmi előzményt tartalmaz az adott tranzakció is. A virtuális világ és a hagyományos üzleti terület metszéspontjaiban is nyomokat hagynak maguk után a felhasználók. A “bevett” valuták és a Bitcoin átváltása során a pénzintézetek adataiban megjelenik az ügyfél, és további azonosítási lehetőséget nyújtanak az áruk hagyományos üzletekben történő adásvétele, a kiszállítási-garanciális ügyintézési adatok, címek valamint a szolgáltatások igénybevételéhez kapcsolódó adatbázisok is.

A hatósági fellépés “királyvize” lehet az FBI eljárása a “Silk Road” weboldal kapcsán. 2013. október 2-án több amerikai hatóság részvételével csaptak le a weboldal üzemeltetőjére. A gyanú szerint többek között droggal, fegyverekkel, illegális gyógyszerekkel és hackerszolgáltatásokkal üzleteltek a weboldal látogatói, az áruk és szolgáltatások ellenértékét többnyire Bitcoinnal egyenlítették ki. A fedett nyomozók 2011. novembere óta több, mint száz tranzakciót hajtottak végre, és a rendelt áruk is többnyire megérkeztek a megadott címre. A felderítést jelentősen elősegítette, hogy az oldal üzemeltetője egy fórumba a saját email címéről írt, így IP címe lenyomozhatóvá -, személyazonossága beazonosíthatóvá vált. Az FBI közel 27000 BTC-t (közel 3,6 millió dollár értékben) foglalt le - mely az ügyfelek pénze volt -, és utalt át saját letéti számlájára. Ez úgy válhatott lehetségessé, hogy a hatóság hozzáfért az ott tárolt “tárcákhoz”, és megszerezték a hozzájuk tartozó jelszavakat is. [51] [52]

Az FBI akciója ellenakciót is indukált: az oldal november 6-án újraindult, és a korábbi erős anonymizálási technikát (TOR hálózat igénybevétele a kommunikációra) még kiegészítették egy PGP-típusú³⁶ titkosítással is. [53]

A számítástechnikai vonzatú bűnelkövetésekhez képes is bonyolultabb, erőforrás-igényesebb a Bitcoin jogellenes, bűncselekményekhez köthető felhasználásának ellenőrzése, felderítése. Önmagában a hálózat forgalmának, a tranzakcióknak a nyomon-követése – az alkalmazott titkosítási megoldás miatt – gyakorlatilag nem lehetséges. A BTC-tulajdonosok kilétének megállapítása csak a fenti-ekben ismertetett körülmények esetén kecsegtet eredménnyel. A hagyományos üzleti szféra felé intézett megkeresésekkel, bevonásukkal, az itt hátrahagyott internetes nyomok összegyűjtésével és elemzésével lehet belépési pontokat találni a Bitcoin világába. Rendkívül erőforrás-igényes statisztikai és forgalmi elemzésekkel lehet feltérképezni a tranzakciós hálózat eseményeit (horizontális) és a tranzakciók előzményeit (vertikális azonosítás). Emellett ki kell dolgozni a tranzakcióelemzés metodikáját és technikáját, mivel a tranzakciók során - igaz csak accountjaikkal, de - azonosítják magukat a résztvevők a teljes hálózat előtt. Mindezen megoldások alapvetően feltételezik a rendvédelmi-felderítési célú beépülést a Bitcoin-hálózatba.

Bár a Bitcoin eddigi - néhányéves - története alapján nem jelenthető ki teljes bizonyossággal, hogy a virtuális fizetőeszköz ezen ideája életképes, és nem jut néhány kevésbé sikeres elődje sorsára, de a létrehozása óta eltelt minden egyes újabb év azt a véleményt erősíti, hogy a Bitcoin megkapaszkodik és egyre nagyobb részt hasít ki magának a világ gazdasági-pénzügyi forgalmából. Ezen forgalom feltehetően jelentős hányada azonban a feketegazdaság tranzakcióinak sikerességét valamint egyéb jogsértő cselekmények "gyümölcsei" gondtalan élvezetét fogja a továbbiakban is biztosítani.

„Alternatív” pénzügyi (tranzakciós) lehetőségek veszélyei

A bemutatott „alternatív” pénzügyi (tranzakciós) lehetőségek több veszélyt is magukban hordoznak. Mint ahogy már arról a bevezetőben is szó volt, ezek a rendszerek teljesen, vagy részben kikerülnek a jelenlegi hivatalos pénzügyi rend-

³⁶ PGP titkosítás: Működése a szimmetrikus és az aszimmetrikus titkosítási módszer kombinációjaként létrejött „hibrid” titkosításon alapul. Először az adatot titkosítja egy véletlen generálású kulccsal, majd a session kulcsot kódolja egy publikus kulccsal. Ezáltal létrejön egy olyan kódolt csomag, amely tartalmazza a titkosított adatot és a visszafejtéshez szükséges kulcsot is. (Bővebben: http://www.piksys.hu/termekek/pgp/npgp_tech.htm)

szert. A részbeni kikerülés azt jelenti, hogy a folyamat bizonyos részeiben valódi pénzmozgások megjelennek teljesen legálisan működő bankoknál is, azonban azok további mozgását (pl. virtuális pénzzé konvertálás után) már nem lehet nyomon követni. Ez pedig alapvetően két dolgot jelent.

Egyrészt – és talán ez a kisebbik, ám pénzügyileg nem elhanyagolandó rész – a korábban említett pénzmozgásokban résztvevők olyan jövedelemre tehetnek szert, amely teljes mértékben kikerülhet az adóhatóság látóköréből. Ez pedig nyilvánvalóan bevételkiesést okoz az adott államnak.

Másrészt – és ez súlyosabb probléma – lehetővé teszi szervezett bűnözők, vagy akár terroristák számára is a pénzmosást. Ennek egyik oka, a már fentebb említett tranzakciók nyomon követhetlensége, azaz egy adott dollár, euro, bármilyen más fizető eszköz útját (pl. „A” személy valódi pénzt vált át virtuális pénzre egy játékban azt átadja „B” személynek, aki visszaváltja valódi pénzre) szinte lehetetlen végig követni. Ha ez még sikerülne is, akkor ott van egy másik, az előzőnél is nagyobb probléma: az ellenőrizhetetlenség. Például a Diablo III-ban valaki saját maga is szerezhethet egy ritka tárgyat (pl. fegyver, páncél stb.), amelyet azután jó pénzért értékesíthet. De nem bizonyítható, hogy valóban ő szerezte-e, kapta, vagy vásárolta valakitől. Mint ahogy az sem bizonyítható, hogy nem ő szerezte. Ma komplett iparágként működik az ilyen tárgyak keresése, majd eladása (pl. Dél-Koreában vagy akár Magyarországon is). [54] Például egy terroristát finanszírozó megvásárolhat egy (vagy sok) értékes tárgyat, majd azt a játék menetében átadhatja (ingyen) a finanszírozottnak. Ő később újraértékesítheti azokat és máris nála van a neki szánt összeg. Ugyanez a szervezett bűnözés esetében lehet a pénz tisztára mosásának egyik lehetősége. Ekkor akár be is vallja az adott személy, hogy neki játékból származik a jövedelme, leadózik utána, ám a pénz valódi eredetét nem lehet felderíteni.

Ellenőrzés hiányosságai

Az alternatív pénzügyi tranzakciókat lehetővé tévő PC/SaaS felhő alapú rendszerek ellenőrzése legalább ugyanolyan kihívást jelent az arra feljogosított nemzetbiztonsági szolgálatoknak és rendvédelmi szerveknek, mint a kommunikációt lehetővé tévőké.

Az első problémát az előbbieket esetében is a jogi hiányosságok jelentik. Egyrészt a virtuális térben megjelent új pénzügyi tranzakciós lehetőségek olyan korábban nem ismert formák, amelyek nem vagy csak óriási beleértéssel férnek bele a jelenlegi pénzügyi, valamint az azokhoz kapcsolódó nemzetbiztonsági, bűnügyi ellenőrzési szabályozásokba. Másrészt ebben a szegmensben is jelentke-

zik a „Felhő alapú rendszerek törvényes ellenőrzési problémái” című cikkben [55] leírt új struktúra, azaz egyre inkább infrastruktúra-, tartalom-, és alkalmazásszolgáltatók alakulnak ki. Az alkalmazásszolgáltatók – amelyek ebben az esetben is lehetnek akár más országban rendes pénzintézetként működő cégek –, úgy tudnak adott esetben külföldről szolgáltatni, hogy semmilyen bejelentési, adófizetési, törvényes ellenőrzést előíró kötelezettségnek nem kell eleget tennie. (pl. PayPal). [56] Harmadrészt pedig ott van még egy nagy probléma, mégpedig az, hogy sokszor az is vita tárgyát képezi, hogy egyáltalán pénzügyi szolgáltatásnak minősül-e az adott tevékenység (pl. BitCoin). [5] Jelenleg nincs olyan legalább a demokratikusnak tekintett országok által elfogadott, irányadónak tekinthető jogszabály, amelyhez Magyarországnak igazodni lehetne. Jellemző példa, hogy az USA-ban új pénzmosás elleni törvényen dolgoznak – többek között a BitCoin miatt –, amelyben a tervezet szerint: „...minden olyan vállalat, ami virtuális pénzt bocsát ki vagy azzal kereskedik, ugyanolyan szabályozás alá kerülne, mint a valódi pénzügyi szolgáltatók. Ezentúl könyvelési kötelezettségük keletkezne és minden 10 ezer dollár feletti tranzakciót be kellene jelenteniük a hatóságoknak.” [57] A tervezet kidolgozói szerint erre azért van szükség, mert a korábban említett lehetőségek, mint pl. a BitCoin egyértelműen elősegítik az illegális gyógyszer- és droggereskedelmet és a nyilvánvaló pénzmosást. [58]

A másik problémát az ellenőrzésre felhasználható technikai eszközrendszerek hiánya okozza. Ez a probléma is több rétegből áll össze. Egyrészt, hogy erre az ellenőrzési feladatra a gyártóknak nincsenek olyan kész megoldásai, mint például a telefonlehallgatásra. Másrészt, még ha találunk is egy adott feladatra megfelelő eszköz(rendszer)t, az alkalmazásszolgáltatók rendkívül heterogén infrastruktúrája okán szinte biztos, hogy ugyanaz egy másik szolgáltatónál már nem használható fel. Mindenhová pedig teljesen új ellenőrző rendszert tervezni és kivitelezni meglehetősen drága mulatság. Harmadrészt pedig az is elképzelhető, hogy a szolgáltató teljes jóindulata mellett sem lehet kinyerni a releváns információkat a rendszeréből, hiszen azt nem ilyen szempontok szerint tervezték. (Például a Diablo III-ban az aukciós házak még egy viszonylag központosított helyet biztosítanak ennek, [59] de egy adott tárgy játékmenet közbeni cseréjét (elejtését, és másik játékos általi felvételét) már rendkívül nehezen (vagy pontosabban fogalmazva leginkább sehogyan sem) lehet követni.)

A fentiekből pedig az következik, hogy a törvényes ellenőrzésre feljogosított szervezeteknek jelenleg más módon kell beszereznie az őket érdeklő információkat. Erre a feladatra léteznek bizonyos eszközök, mint azt a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata” I. és II. című cikkek is leírták. [60] [61] Azokban a cikkekben található elemzés és az ott megfogalmazott kö-

vetkeztetések ebben az esetben is helytállóak, azaz több módszer is az említett szolgáltatók rendelkezésére áll. Azonban ezek mindegyikének megvannak a maga hátrányai és egyik sem teszi lehetővé a célszemélyek releváns adatainak, forgalmainak 100 %-os kinyerését. Ráadásul nem is a fentebb vázolt pénzügyi tranzakciók ellenőrzéséhez tervezték azokat, bár kétség kívül számtalan közvetett és közvetlen adatot is képesek lehetnek szolgáltatni. Van olyan ország is (Kína), ahol a problémát törvényi szabályozással kívánják megoldani, azaz egyszerűen betiltják virtuális fizetőeszközök valós pénzre történő átváltását. [62] [63]

Megjegyzendő, hogy az online játékoknál is megindult egyfajta önszabályozás a pénzügyi tranzakciók tekintetében. A World of Warcraft esetében megjelentek olyan – ritka ezért rendkívül értékes – tárgyak, amelyek un. lélekhez kötöttek, azaz csak az játékos használhatja, aki megtalálta, az másnak nem adható át. [64] Tovább korlátozza a pénzmozgást, hogy bizonyos tárgyak csak adott szerveren belül osztható meg. Bár ez utóbbi könnyen kijátszható pl. a helyi virtuális „aranyra” váltással és annak átadásával. A League of Legends nevű játékban például úgy korlátozták a különböző „ajándékok” átadását, hogy azok tranzakcióját előzetes „barát” megjelöléshez kötötték, és a jelölést követően legalább két hét várakozási időhöz. További korlátozás, hogy az átadónak legalább 20-as szintű, az átvevőnek pedig legalább 10-es szintűnek kell lennie, valamint egy nap maximum 3 tárgy adható át. [65] Bár ezt elsősorban az élvezetesebb játékmenetért (elsősorban a kezdők, kevesebbet játszóknak kedvéért) alakították ki, de adott esetben nagymértékben segítheti egy célszemély kapcsolati körének feltérképezését, vagy adott esetben akár a tranzakciók megakadályozását is. A Diablo III-ban – szintén az élvezetesebb játékmenetért és nem utolsó sorban az üzletszerű, iparként működő tárgy”farmolások” visszaszorítása miatt bejelentették, hogy az aukciós házat meg fogják szüntetni. [66]

Ezek a korlátozások csökkentik, de nem teszik lehetetlenné a korábban említett illegális pénzügyi tranzakciókat, ugyanakkor a törvényes ellenőrzést végzők számára a nyomon követhetőséget valamelyest elősegítik. Mindenesetre már valamiféle előrelépést jelentenek a nemzetbiztonsági szolgáltatók és a rendvédelmi szervek titkos információgyűjtő és titkos adatszerző feladatainak végrehajtásához.

Összefoglalás, következtetések

A PC/SaaS felhő alapú rendszerek által biztosított új, alternatív pénzügyi tranzakciós lehetőségek mindamelllett, hogy teljesítik a fejlesztők által kitalált funkciókat, veszélyeket is magukban hordoznak. Olyan új lehetőséget teremtenek

pénzmosásra, terrorizmus finanszírozására, és nem utolsósorban be nem vallott jövedelemszerzésre, amelyekkel korábban az ezek ellen fellépő nemzetbiztonsági szolgálatok, rendvédelmi szervek és adóhatóságok nem találkoztak. Így ezen rendszerek ellenőrzésének igénye – a felhasználás növekedésével – egyre sürgetőbbben merül fel, ugyanakkor ennek jelenleg jogi, és technikai korlátai is vannak.

Napjainkra a virtuális világ - és benne a Bitcoin - valós alternatívájává és versenytársává vált a hagyományos megoldásoknak, így a rendvédelmi-felderítési tevékenységnek is ki kell terjednie erre az élettérre is. Jelentős pénzügyi-gazdasági potenciállal rendelkező államok - így az Amerikai Egyesült Államok, Anglia, Németország már megkezdték az elkerülhetetlenné váló szabályozás előkészítését.

A virtuális fizetőeszközök problematikája, mint lakmuszpapír ráirányítja a figyelmet arra is, hogy az új internetes technológiák, szolgáltatások komplex, és ágazatonkénti áttekintése és szabályozása tovább már nem halogatható.

Jelen cikkből levonható következtetések:

1. A virtuális világban új, a korábbi pénzügyi rendszerhez kapcsolódó, de azt mégis elkerülő rendszerek jöttek létre, amelyekkel pénzügyi tranzakciók bonyolíthatók.
2. Ezen tranzakciók ellenőrzése ugyanolyan fontos a törvényes ellenőrzést végző szolgálatok számára, mint a klasszikus pénzügyi tranzakcióké.
3. Ezen rendszerek ellenőrzése minden ország törvényes ellenőrzést végző szervei számára kihívást jelentenek.
4. Ezen rendszerek ellenőrzésére – akár csak más, például elektronikus úton folytatott kommunikációt lehetővé tevő PC/SaaS felhő alapú rendszerekére – nincsen olyan általánosan elfogadott jogi szabályozás a ellenőrzése kapcsán, amelyhez – akár Magyarországnak is – igazodni lehetne.
5. Az felhatalmazott szolgálatok ugyan rendelkeznek olyan módszerekkel, eszközökkel, amelyek – bizonyos mértékig – lehetővé teszik az ellenőrzést, de ezek – miután nem erre a problémára készültek – csupán korlátozott eredményt adnak. Így a szükséges információk megszerzését más módszerekkel (pl. HUMINT) is hatékonyan támogatni szükséges.
6. Mihamarabb meg kell hozni a törvényi kereteket, amiben definiálni kell az alkalmazásszolgáltatók fogalmát úgy, hogy abba a fent említett pénzügyi tranzakciókat lehetővé tévő rendszerek is beleérthetők legyenek.

7. Magyarországnak – akárcsak a többi országnak – pénzügyi érdeke is, hogy az alkalmazásszolgáltatók hazai működését mihamarabb más szolgáltatókhoz hasonló jogi keretek közé terelje. Így a cégekkel egyrészt a megfelelő adók, járulékok stb. megfizettethetők, másrészt a felhasználók adatainak elérése lehetőséget teremt jelenleg nem adózó jövedelmek feltérképezéséhez is.

Annak érdekében, hogy az új pénzügyi tranzakciós lehetőségeket biztosító PC/SaaS felhő alapú rendszerek törvényes ellenőrzési problémáit kezelni lehessen, ugyanazokat a lépéseket kell megtenni, mint amelyek a „Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata” II. című cikkben a kommunikációt lehetővé tevő rendszerekkel kapcsolatban megfogalmazásra kerültek. Az az további feladatként, a jogi szabályozás kialakítása előtt, el kell végezni az infrastruktúra-, alkalmazás- és tartalomszolgáltatók fogalmának a definiálását. Ezt követően lehet meghatározni, hogy mit kell ellenőrzés alá vonni ahhoz, hogy a nemzetbiztonsági és a bűnüldözői munkát hatékonyan lehessen a támogatni, és ezek alapján célszerű a törvényi szabályozást átalakítani.

Felhasznált irodalom

- [1] http://www.libri.hu/cikk/fizetes_es_szallitas (2013.10.22.)
- [2] <https://www.otpbank.hu/portal/hu/fooldal> (2013.10.22.)
- [3] <http://en.support.wordpress.com/bitcoin/> (2013.10.22.)
- [4] <https://www.paypal.com/hu/webapps/mpp/home> (2013.10.22.)
- [5] Mi is az a Bitcoin? http://bitcoin.hu/?page_id=167 (2013. 11. 23.)
- [6] VOITH Hunor: Pénzmosással vádolják a Bitcoin Alapítvány alelnökét (2014. 01. 28.)
http://itcafe.hu/hir/penzmosassal_vadoljak_a_bitcoin_alapitvany_alelnok.html (2014. 02. 27.)
- [7] TRAVIS Green: Send money to friends with Gmail and Google Wallet
<http://googlecommerce.blogspot.hu/2013/05/send-money-to-friends-with-gmail-and.html> (2013.10.21.)
- [8] Send and receive money from anywhere
<http://www.google.com/wallet/send-money/> (2013.10.22.)
- [9] SZENTENDREI Lajos: Arab „hadjárat” Svájcban. HetiVálasz.hu (2013.07.28.)
<http://hetivalasz.hu/uzlet/az-erintett-bankok-eddig-egyetlen-mukkotsem-szoltak-a-banktitokra-hivatkozva-haritanak-el-mindenfele-kommentart-59931> (2013.10.22.)

- [10] tucano: A svájci banktitok - I. rész (2011.03.28.)
http://lemil.blog.hu/2011/03/28/a_svajci_banktitok (2013.10.22.)
- [11] VÁMOSI-NAGY: nem könnyű Svájcot rávenni a banktitok feltörésére. ma.hu (2013.01.16.)
http://www.ma.hu/belfold/158062/VamosiNagy_nem_konnyu_Svajcot_ravenni_a_banktitok_feltoresere (2013.10.22.)
- [12] DAJKÓ Pál: A Google továbbra sem ad ki adatokat a magyar kormánynak (2013. 01. 24.)
http://itcafe.hu/hir/google_atlathatosag_transparency.html (2013. 02. 09.)
- [13] <https://www.otpbank.hu/direktdemo/hu/bankszamla-nyito> (2013.10.26.)
- [14] <https://www.otpbank.hu/direktdemo/hu/utalasok> (2013.10.26.)
- [15] Már csak négy órán át vándorol a pénz. (2012. 07. 01.)
- [16] <https://www.paypal-europe.com/magyar/> (2013. 11. 25.)
- [17] <http://online-fizetes-magyarul.info/neteller/neteller.html> (2013. 11. 25.)
- [18] <http://online-fizetes-magyarul.info/> (2013. 11. 25.)
- [19] P2P-finanszírozás szorítja ki a bankokat a hitelezésből
http://sg.hu/cikkek/101294/p2p_finanszirozasa_szoritja_ki_a_bankokat_a_hitelezesbol (2013. 11. 25.)
- [20] Stan STALNAKER: Bitcoin, Ven, és a hagyományos pénz vége
<http://bitcoin.hu/?p=1228> (2013. 11. 25.)
- [21] A Bitcoin csak a kezdet, itt a Dogecoin - egyre több a virtuális pénz (2014. 02. 03.) <http://www.vg.hu/penzugy/a-bitcoin-csak-a-kezdet-itt-a-dogecoin-egyre-tobb-a-virtualis-penz-420897> (2014.02.03.)
- [22] http://bitcoin.hu/?page_id=1456 (2014.02.03.)
- [23] ESZE Dóra: Bitcoin, a forradalmi valuta (2013. 10. 09.)
<http://www.uzletresz.hu/penzugy/20131009-bitcoin-a-forradalmi-valuta.html> (2013. 10. 09.)
- [24] TURZÓ Ádám Pál: Megint eldurant egy Bitcoin-lufi - Mi áll a háttérben? (2013. 10. 27.)
http://www.portfolio.hu/vallalatok/it/megint_eldurant_egy_bitcoin-lufi_mi_all_a_hatterben.190922.html (2013. 10. 27.)
- [25] Ők is a Bitcoinból gazdagodtak meg (2013. 11.15.)
http://index.hu/tech/2013/11/15/ok_is_a_bitcoinbol_gazdagodtak_meg/ (2013.11.15.)

- [26] A pénzvilág nagyjai alig értik a Bitcoin – és félnek kérdezni (2013. 07. 04.) <http://www.hirado.hu/2013/07/04/a-penzvilag-nagyjai-alig-ertik-a-bitcoin-es-felne> (2014. 02. 26.)
- [27] Hivatalosan is pénz a Bitcoin (2013. 08. 09.) http://index.hu/tech/2013/08/09/hivatalosan_is_penz_a_bitcoin/ (2013.08.09.)
- [28] VOITH Hunor: Igazi valutának minősítette a Bitcoin egy amerikai szövetségi bíró (2013. 08. 08.) http://itcafe.hu/hir/a_bitcoin_igazi_penz_egy_amerikai_biro_szerint.html (2013.08.08.)
- [29] VOITH Hunor: Betiltották Oroszországban a digitális valuták használatát (2014. 02. 10.) http://itcafe.hu/hir/oroszorszag_betiltotta_a_digitalis_valutakat_bitco.html (2014.02.10.)
- [30] WIEZNER István: Betiltották Thaiföldön a Bitcoin (2013. 07. 30.) <http://pcworld.hu/kozelet/betiltottak-thaifoldon-a-bitcoin.html> (2014.02.10.)
- [31] VOITH Hunor: A kínai kormány, a Francia Nemzeti Bank és Alan Greenspan nekiment a Bitcoinnak (2013. 12. 06.) http://itcafe.hu/hir/bitcoin_kina_francia_nemzeti_bank_alan_greenSPAN.html (2013.12.06.)
- [32] Megint eldurant egy Bitcoin-lufi - Mi áll a háttérben? (2013. 10. 27.) <http://hunnio.com/news.php?readmore=669> (2014. 02. 27.)
- [33] Megint mosolyoghatnak a Bitcoin-tulajdonosok (2013. 11. 14.) http://www.portfolio.hu/vallalatok/it/megint_mosolyoghatnak_a_bitcoin-tulajdonosok (2014. 02. 27.)
- [34] Itt már lakbért is lehet virtuális pénzzel fizetni (2013. 04. 09.) http://hvg.hu/ingatlan/20130409_Itt_mar_virtualis_penzzel_is_lehet_lakberet (2014. 02. 27.)
- [35] Itt az első bébi, akiért virtuális pénzzel fizettek (2013. 06. 11.) http://hvg.hu/gazdasag/20130611_Itt_az_elso_bebi_akiert_virtualis_penzzel (2014. 02. 27.)
- [36] <http://lamassubtc.com/#contact> (2013.07.26.)
- [37] KERNER Zsolt: Itt a Bitcoin vége? <http://444.hu/2013/05/06/mi-a-fasz-az-a-bitcoin/> (2013. 11. 23.)

- [38] http://blockchain.info/hu/charts/market-price?timespan=1year&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address= (2013. 12. 21.)
<http://www.origo.hu/gazdasag/20120701-mostantol-negy-ora-alatt-atutalodik-a-penz-napkozbeni-atutalasi-rendszer.html> (2013.10.26.)
- [39] A bitcoin, mint megtakarítás
<http://hu.falkvinge.net/2011/05/29/a-bitcoin-mint-megtakaritas/> (2013. 05. 29.)
- [40] Want to rent an 80-120k DDoS Botnet?
<https://blog.damballa.com/archives/330> (2014. 02. 27.)
- [41] Botcoin: Bitcoin Mining by Botnet
<http://krebsonsecurity.com/2013/07/botcoin-bitcoin-mining-by-botnet/> (2014. 02. 27.)
- [42] JIM FINKLE: 'Pony' botnet steals bitcoins, digital currencies: Trustwave. (2014. 02. 24.) <http://www.reuters.com/article/2014/02/24/us-bitcoin-security-idUSBREA1N1JO20140224> (2014. 02. 27.)
- [43] Bitcoin, Scribd (2013.04.05.)
http://buhera.blog.hu/2013/04/05/bitcoin_scribd (2014. 02. 27.)
- [44] Louis Goddard: Bitcoin exchange BitFloor suspends operations after \$250,000 theft. (2012. 09. 05.)
<http://www.theverge.com/2012/9/5/3293375/bitfloor-bitcoin-exchange-suspended-theft> (2014. 02. 27.)
- [45] Bitcoin Hit By 'Massive' DDoS Attack As Tensions Rise. (2014. 02. 12.)
<http://www.forbes.com/sites/leoking/2014/02/12/bitcoin-hit-by-massive-ddos-attack-as-tensions-rise/> (2014. 03. 02.)
- [46] MATTHEW Boesler: WORLD'S LARGEST BITCOIN EXCHANGE: We Are Suffering A Massive Attack On Our Servers. (2013. 04. 04.)
<http://www.businessinsider.com/ddos-attack-on-mt-gox-bitcoin-servers-2013-4> (2014. 03. 02.)
- [47] How does blockchain.info's mixing service work?
<http://bitcoin.stackexchange.com/questions/8232/how-does-blockchain-infos-mixing-service-work> (2013.03.08.)
- [48] <https://bitlaunder.com> (2014. 02. 27.)
- [49] <http://app.bitlaunder.com> (2014. 02. 27.)
- [50] Cyrus Farivar: Névtelenségi figyelmeztetés Írországból (2011. 07. 31.)
<http://bitcoin.hu/?p=646> (2014. 02. 27.)

- [51] Az FBI lecsapott a web sötét oldalára (2013. 10. 03.)
http://index.hu/tech/2013/10/03/az_fbi_lecsapott_a_web_sotet_oldalara/ (2014. 02. 27.)
- [52] VOITH Hunor: Vajon merre van a Silk Roadtól elkobzott Bitcoin? (2013. 10. 04.)
http://itcafe.hu/hir/silk_road_fbi_bitcoin_elkobzas_tor_blummer.html (2014. 02. 27.)
- [53] Újraindult a hírhedt online drogpiac. (2013. 07. 11.)
<http://www.karpatinfo.net/cikk/kriminalis/ujraindult-hirhedt-online-drogpiac> (2014. 02. 27.)
- [54] Mocsy: Aranyparaszt voltam a Diablo III-ban. Hogyan lehet pénzt keresni játékkal? Mert tényleg lehet. GameStar (2012. 10. 22.)
<http://www.gamestar.hu/8222aranyparaszt8221-voltam-a-diablo-iii-ban.html> (2013. 10.22.)
- [55] Kovács Zoltán: FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI PROBLÉMÁI Hadmérnök, VIII. Évfolyam 1. szám - 2013. március
- [56] <http://www.cashmaker.hu/netbankok/paypal/> (2014. 03. 02.)
- [57] DOJCSÁK Dániel: Ellenőrizné az USA a virtuális pénzeket (2013. 03. 25.)
<http://www.hsw.hu/hirek/50009/bitcoin-virtualis-penz-fbi-illegalis-penzmosas.html> (2013.07.02.)
- [58] JEFFREY SPARSHOTT: Web Money Gets Laundering Rule
<http://online.wsj.com/article/SB10001424127887324373204578374611351125202.html> (2013.07.02.)
- [59] <http://us.battle.net/d3/en/game/guide/items/auction-house> (2013.10.22.)
- [60] Kovács Zoltán: FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREI VIZSGÁLATA I. RÉSZ Hadmérnök, VIII. Évfolyam 3. szám - 2013. szeptember
- [61] Kovács Zoltán: FELHŐ ALAPÚ RENDSZEREK TÖRVÉNYES ELLENŐRZÉSI MÓDSZEREI VIZSGÁLATA II. RÉSZ Hadmérnök, VIII. Évfolyam 3. szám - 2013. szeptember
- [62] Thomas CLABURN: China Limits Use Of Virtual Currency. InformationWeek (2009. 06. 29.)
<http://www.informationweek.com/internet/ebusiness/china-limits-use-of-virtual-currency/218101859> (2013. 10.23.)

- [63] Chavalier: Kína betiltja a gold farmolást! GameStar (2009. 07. 01.)
<http://www.gamestar.hu/kina-betiltja-a-gold-farmolast.html> (2013. 10. 23.)
- [64] World Of Warcraft: Világok harca. mindenkilapja.hu
<http://wow500.mindenkilapja.hu/html/18900252/render/> (2013. 10. 23.)
- [65] <https://support.leagueoflegends.com/entries/23111872-Gifting-Guide-and-FAQ> (2013. 10. 25.)
- [66] John HIGHT: Diablo® III Auction House Update. (2013. 09. 17.)
<http://us.battle.net/d3/en/blog/10974978/> (2013.10.23.)