Első megjelenés

Tüzes Marcell

Bitcoin – A pénz új formája

1. BEVEZETÉS

Az *Infokommunikáció és jog* 49. számában Eszteri Dániel mutatta be a folyóirat olvasóinak a Bitcoin névre hallgató elektronikus fizetőeszközt *Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze?* című cikkében.[1] Jelen írásom célja, hogy Eszteri írásához kapcsolódva, azt kiegészítve ismertessem meg az olvasót a Bitcoin néhány gazdasági és műszakibb jellegű vetületével, valamint, hogy beszámoljak az előző cikk óta történt néhány említésre méltó eseményről.

2. EGY ÚJ PÉNZ KEZDETE

A Bitcoin egy anonim, nyílt forráskódú, interneten használható virtuális pénzeszköz. A korábbi elektronikus pénzeszközökkel szemben a Bitcoin tranzakciók jóváhagyása a hálózaton elosztva, peer-to-peer technológiával történik, így nincs szükség központi szabályozó testületre, ami a pénzeszköz értékét változtathatná vagy a felhasználókat szankcionálhatná.

A Bitcoin egy *crypto-currency*, melynek koncepcióját 1998-ban Wei Dai fektette le. Crypto-currencynek olyan digitális valutákat nevezhetünk, amelyek különböző kriptográfiai eljárásokra épülve védik a fizetőeszköz biztonságát és nehezítik meg a hamisítást. Wei Dai-t a crypto-anarchia nevű utópisztikus koncepció ihlette meg, és egy utópisztikus jövő lehetséges pénzét írta le *b-money* névre hallgató protokollvázlatában[2].

A blokk az az egység, amelybe a még jóvá nem hagyott tranzakciókat összegyűjtik, és ezt új láncszemként fűzik hozzá a már meglévő blokklánchoz.

Satoshi Nakamoto 2008. október 31-én publikálta tanulmányát, mely Wei víziójának gyakorlati megvalósítását írja le[3]. Satoshi ekkorra már regisztrálta a *www.bitcoin.org* webcímet és javában dolgozott a felvázolt rendszer megvalósításán. A Satoshi Nakamoto álnév mögött megbújó fejlesztő (vagy fejlesztők) 2009 januárjában indította el a működő rendszert, az első Bitcoin blokk (vagyis a genezis blokk) generálása 2009. január 3-án történt[4].

3. A BITCOIN MŰKÖDÉSE

3.1. A Bitcoin blokklánc

A Bitcoin használatához internetkapcsolatra, virtuális pénztárcánk kezeléséhez kliensprogramra, valamint értelemszerűen ezek használatához számítógépre vagy fejlettebb mobiltelefonra van szükségünk. Személyi számítógépeken a *www.bitcoin.org* címen elérhető, eredetileg Satoshi által fejlesztett „hivatalos" kliens a legelterjedtebb, de különböző platformokra és speciális felhasználásokra tucatnyi alternatív kliens is létezik.

A Bitcoin gerince a blokklánc. Ez gyakorlatilag egy adatbázis, amellyel minden felhasználó rendelkezik, és tartalmazza az összes eddig lezajlott tranzakciót. Ezáltal minden egyes felhasználó láthatja nem csak azt, hogy a rendszerben létező Bitcoin érmék adott pillanatban melyik címhez tartoznak, hanem vissza is tudja követni azok összes tranzakcióját, egészen az érme generálásáig, létrejöttéig. Az adatbázis megtekintéshez az átlag felhasználóénál magasabb programozási ismeretek szükségesek, ezért a teljes adatbázis online is elérhető, böngészhető és kereshető formában.[5]

A blokk tehát az az egység, amelybe a még jóvá nem hagyott tranzakciókat összegyűjtik, és ezt új láncszemként fűzik hozzá a már meglévő blokklánchoz. Egy blokk fix méretű fejlécből és változó méretű tartalmi részből áll. A fejlécbe kerülnek a blokk információi, így például az érvényesség ellenőrzéséhez szükséges adatok. A blokk tartalmi részébe kerül a hálózaton közzétett érvényes tranzakciók azon része, amit a blokk generálója belefoglal. A frissen közzétett tranzakciók többsége az első vagy második adandó alkalommal a következő generált blokk részévé válik, vagyis 10–20 percen belül a blokklánc része lesz, de protokoll ezt nem köti ki, így előfordul olyan, hogy órák is eltelnek a blokkba foglalásig.[6] A felhasználó dönthet úgy, hogy a tranzakció összegén felül egy tranzakciós díjat is hajlandó fizetni, ezzel növelve a tranzakció blokkba foglalásának esélyeit. A blokk első tranzakciója mindig egy különleges tranzakció, amely egy meghatározott összeget (jelenleg 50 BTC) jutalmaz a blokk generálójának.[7]

A blokklánc kifejezés arra utal, hogy a blokkok közt szigorú egymásutániság áll fenn, amit a rendszer úgy biztosít, hogy minden blokk fejléce tartalmazza az őt megelőző blokk hash-ét. Mindig az a leghosszabb blokklánc az érvényes, amelyen belül minden blokk érvényes, és a lánc a genezis blokkal kezdődik.

A blokkláncban minden érméhez tulajdonosának nyilvános kulcsa van hozzárendelve. A tranzakciók gyakorlatilag üzenetek, amelyekben az érmék előző gazdája az érmékhez rendeli azok új gazdájának nyilvános kulcsát, és a tranzakció érvényesítése érdekében saját titkos kulcsával írja alá azt.[8]

3.2. Bányászás

A rendszer azon szereplőit, akik számítógépeik számítási tudását az új blokkok generálására szentelik, bányászoknak nevezzük. A bányász feladata, hogy a tranzakciókat összegyűjtse, és azokat számítási feladatok elvégzésével jóváhagyja. Ezért a munkáért cserébe a rendszerben előre kódolt mennyiségű jutalomösszeget, valamint ezen felül a tranzakciókat kezdeményezők által opcionálisan fizetett tranzakciós díjakat kapja. Persze nem csak egy bányász van a hálózatban, így versenyhelyzet alakul ki, ahol a véletlen számok alkalmazása miatt bárki nyerhet, azonban a nagyobb számítási kapacitással rendelkező bányászok nyilván nagyobb eséllyel generálnak blokkot és kaparintják meg a jutalom Bitcoin összeget és a tranzakciós díjakat.

A Budapesti Corvinus Egyetem hallgatója, bachelor szakdolgozatának témája a Bitcoin.

A blokkgenerálás rendszerességének megtartása érdekében a nehézségi szintet minden 2016 blokk legenerálása után újra meghatározza a beépített algoritmus. A cél, hogy átlagosan 10 percenként jöjjön létre egy új blokk, így ez alapján 2016 blokk létrejöttének pontosan 2 hétig kell tartania; amennyiben ennél rövidebb idő alatt történt, úgy a nehézségi szint emelkedik, ellenkező esetben csökken. Így a Moore-törvényében megfogalmazott exponenciális számítási kapacitás növekedés nincs hatással a generálás gyorsaságára.[9]

A blokkgeneráláshoz komoly számítási kapacitásra van szükség. Az ilyen kriptográfiai jellegű feladatok megoldására a videokártyák grafikus processzorai a legalkalmasabbak. A Bitcoin bányászok gyakran drága, nagy teljesítményű videokártyákba ruháznak be, és a több grafikus kártya felhasználásával épített célszámítógépek sem ritkák.

Digitális javaknál felmerül egy probléma, ami a fizikai formában létező eszközöknél nem. Egy adott pénzérme vagy bankjegy csak egyvalaki tulajdonában lehet (itt fizikai tulajdonlásról beszélünk). Digitális javakat azonban korlátlan mennyiségben másolhatunk, így több, az eredetivel egyező másolatpéldány jöhet létre. Nyilvánvaló, hogy ha egy digitális pénzről beszélünk, akkor nem engedhető meg, hogy ugyanazt az érmét valaki több helyen is elköltse, és ezáltal egynél több személy birtokolja. Ennek megoldására a Bitcoin rendszerben a résztvevők csak azt a tranzakciót fogadják el érvényesként egy adott érme elköltésére, amelyik időben előbb következett be.

3.3. Kriptográfia

A kriptográfia rejtjelzéssel, titkosírásokkal és kódolással foglalkozó tudományág. A Bitcoin protokoll esetében egy sor kriptográfiai művelet biztosítja a rendszer biztonságos működését. A felhasznált módszerek közt szerepel nyilvános kulcsú rejtjelezés és hash eljárások használata. A nyilvános kulcsú rejtjelezésben a felhasználóknak matematikailag összefüggő titkos és nyilvános kulcspárjaik vannak. A nyilvános kulcsból nem fejthető vissza a titkos kulcs, így az nyilvánosan terjeszthető. Egy adott nyilvános kulccsal kódolt üzenetet csak a hozzá tartozó titkos kulccsal lehet visszafejteni. A hash eljárások tetszőleges hosszúságú adatot egy előre megadott hosszúságúra képeznek le. A bemeneti adat legapróbb változásának is jelentős változást kell okoznia a hash eredményében, így megfelelő alkalmazás esetén ez kiváló módszer adatok egyezőségének vizsgálatára.

A felhasználó gyakorlatilag nem a Bitcoin érméket birtokolja, csak az azok felhasználásához szükséges titkos kulcsokat.

Most tehát röviden lássuk, hogy hogyan működik a Bitcoin kriptográfiai szempontból: Amikor egy érmét átutalnak egy új gazdához, az eddigi tulajdonos létrehoz egy üzenetet – a tranzakciót –, melyben az új tulajdonos nyilvános kulcsát hozzárendeli az utalni kívánt összeghez, és ezt az üzenetet saját titkos kulcsával írja alá. Ezekhez a lépésekhez a rendszer az ECDSA kulcsokat használja. A Bitcoin-cím a nyilvános kulcs hash-e, míg a titkos kulcsot mindenki a saját számítógépén tárolja virtuális pénztárcájában, a kliensprogram által létrehozott wallet.dat fájlban. A felhasználó tehát gyakorlatilag nem a Bitcoin érméket birtokolja, csak az azok felhasználásához szükséges titkos kulcsokat.

A Bitcoin címek előállítása több hash művelet egymásba ágyazásából áll. Egy 65 byte-os nyilvános kulcson SHA-256, majd RIPEMD-160 hash-t alkalmaznak, valamint ehhez további két, egymásba ágyazott SHA-256 hash-t generálva ellenőrző összeget fűznek. Az így kapott karaktersorból egy base58 típuskonverzió során többek közt kiszűrik a szóközöket és a könnyen összetéveszthető 0OIl karaktereket. Ezzel előáll az átlag 33 karakterből álló, 1-essel kezdődő Bitcoin cím. Példa Bitcoin címre: 157JU5xkmE8WCUkxtqo BPSf8cb8pnTAQSR.

A blokkgenerálás során az SHA-256 hash algoritmust használják. A bányász begyűjti a tranzakció üzeneteket és azokat egy blokkba foglalja. Ahhoz, hogy a blokk érvényes legyen, meg kell találnia a megoldást egy nehéz számítási feladatra: addig kell véletlen biteket hozzáadnia a generálni kívánt blokkhoz és ebből inverz SHA-256 hash műveleteket végeznie, amíg nem talál egy olyan megoldást, ami megfelel a hálózat résztvevői által előre meghatározott nehézségi szintnek.[10]

3.4. Egyéb felhasználási módok

A nyílt programkód lehetőséget ad arra, hogy a Bitcoin blokkláncának elvén alapuló, annak részletein változtató alternatív projektek (pl. namecoin, litecoin, solidcoin, testnet) jelenjenek meg. Ezek egy jelentős része nem valós használatra, hanem inkább különböző teóriák tesztelésére és demonstrálására íródik. Az elvi lehetősége azonban adott annak, hogy a felhasználók tömegével pártoljanak át ezek valamelyikéhez, így nemcsak a Bitcoin felhasználók számát csökkentve, hanem konkurenciát is teremtve annak.

Említésre méltó a Namecoin, ami egy ígéretes blokklánc alapú technológia, amelyben szabadon választott értékek fűzhetők az egyes érmékhez. A Namecoin így például elláthat DNS[11] feladatokat, megfelelően konfigurált webböngészővel már használhatóak az ezen alapuló .bit kiterjesztésű domain nevek[12]. Ugyancsak alkalmazható például a nehezen megjegyezhető Bitcoin címek könnyen felidézhető formára hozásában.

Számos alternatív projekt teljesen megtartja a Bitcoin működésének logikáját, így például a Litecoin ami mindössze a blokkgenerálás gyakoriságában tér el elődjétől, így ebben a láncban 2.5 percenként jön létre új blokk.

4. A RENDSZER TULAJDONSÁGAI

4.1. Anonimitás

A Bitcoin legtöbbször hangoztatott tulajdonsága az anonimitás. De vajon mit takar ez az anonimitás? Mitől lesz anonim egy pénzeszköz?

A jelenleg használt, érme és papír alapú készpénzek igen magas anonimitási faktorral rendelkeznek, vagyis nehéz őket egyértelműen egy személyhez kötni. A papírpénzek egyedi azonosítókkal rendelkeznek, amelyek alapján részlegesen követhető egy adott papírpénz útja.

A skála másik végén állnak a banki tranzakciók, ahol a számla tulajdonosa a bank számára ismert és jól beazonosítható, és egy hatósági eljárás esetén a személyazonosságra vonatkozó információkat a bank a hatóságok rendelkezésére bocsátja.

Senki nem szeretné, hogy egy harmadik személy a tranzakcióit fel tudja térképezni. Ez nyilván kiemelkedően fontos azok számára, akik valamilyen illegális tevékenységet végeznek, de a jogkövető magatartást tanúsító átlagember se örül, ha valaki túlságosan belelát, honnan szerzi vagy mire költi a pénzét. A Bitcoin pont az előbbiek miatt lett kiemelten népszerű a Nagy Testvér mindent látó szemei elől menekülni vágyó anarchisták, a drogkereskedők, az adócsalók, valamint egyéb megkérdőjelezhető legalitású tevékenységeket folytatók körében.

A Wikileaks nevű, leginkább titkosított kormányinformációk kiszivárogtatására specializálódott, adományokból működő weblap 2010 decemberében szembesült azzal a problémával, hogy a VISA, a MasterCard, a PayPal, a Western Union és a Bank of America pénzügyi szolgáltatók befagyasztották számláit, így próbálva ellehetetleníteni a működését. A Wikileaks 2011 júniusától Bitcoin támogatást is elfogad, ezzel próbálva helyettesíteni a letiltott támogatási csatornák egy részét.[13] A Bitcoin kvázi-anonimitása ilyen helyzetekben kifejezetten előnyös az adományozóknak, hiszen gyanítható módon többségük nem szeretné, ha visszakereshető lenne.

Egy másik, nagy visszhangot keltő téma a Bitcoinnal és annak anonimitásával kapcsolatban a Silk Road ügye. A Silk Road névre hallgató online felületet az illegális drogok Amazon.com-jaként jellemzik, melynek eléréséhez szükség van a TOR nevű titkosított, anonim hálózatot létrehozó rendszerre. A Silk Road egyetlen elfogadott fizetőeszköze a Bitcoin, amiért illegális tudatmódosító szerek tucatjai közül válogathatnak az érdeklődők.[14] Az anonimitás szempontjából az egyetlen gyenge pont, hogy a megvásárolt tudatmódosítókat postai úton küldik el a vásárlóknak. A Silk Road akkor vált igazán ismertté, amikor 2011 nyarán két amerikai demokrata szenátor levélben hívta fel Eric Holder amerikai igazságügy-miniszter és a DEA[15] figyelmét a piactér, valamint a Bitcoin veszélyeire.[16] A levél felkeltette az online és offline médiumok érdeklődését, rengeteg neves magazin értekezett a témáról, ami nem csak a Silk Road és Bitcoin felhasználók számát növelte számottevően, hanem ezzel a Bitcoin árfolyamát is.

Bármelyik kliensprogrammal, egyetlen gombnyomással generálhatunk magunknak új Bitcoin címet, ehhez nincs szükségünk semmilyen személyes adat megadására, és ez nem tartalmaz olyan információt, amivel az adott címet generáló számítógép vagy mobil eszköz beazonosítható lenne.

Attól kezdve, hogy ezt a címet először tranzakcióban használjuk, a blokklánc részévé válik. Mivel a blokklánc publikus, így bárki láthatja, hogy az adott címen mikor, milyen értékű tranzakciók mentek végbe és ezek honnan

vagy hová érkeztek. Tehát a pénz áramlása mindenki előtt nyilvános, az azonban nem, hogy az adott számla kié.

Egy 2011 júliusában végzett kutatás a júniusban történt „lopáson" keresztül vizsgálta a Bitcoin anonimitását. Pontosan az anonimitás miatt kell a lopást is feltételesen kezelni, mivel nem kizárható, hogy a tolvaj és a károsult ugyanaz a személy. A kutatás a címek azonosításához először is begyűjtötte az egyértelműen egy meghatározott felhasználóhoz rendelhető címeket, ezek például a különböző Bitcoin szolgáltatások (szerencsejátékok, eWallet), az adományt elfogadó szervezetek/weblapok (Wikileaks, Bitcoin faucet) és a nyilvános fórumokon (pl. *bitcointalk.org*) a felhasználók által önként megosztott címek. Az ismert címek birtokában a tranzakciókat vizsgálták különböző hálózatelemzői technikákkal, és megállapították, hogy a Bitcoin rendszer szereplőinek jelentős része beazonosítható, továbbá nagy eséllyel megállapítható különböző Bitcoin címekről, ha ugyanahhoz a személyhez tartoznak.[17]

A tranzakciók követhetőségének nehezítésére lehetőség van mixer szolgáltatások alkalmazására. Ezek lényege, hogy a különböző felhasználóktól érkező tranzakciókat más felhasználók hasonló célú pénzéből elégíti ki, így összekuszálva és nehezebben követhetővé téve a tranzakciók útját.

4.2. Biztonság

Joggal merül fel a kérdés, hogy mennyire biztonságos a Bitcoin technikai oldalról.

A Bitcoin rendszernek sosem készült átfogó dokumentációja, ehhez legközelebb a *bitcoin.it* webcímen elérhető wiki áll, ám az itt megtalálható leírások közel sem tekinthetők teljesnek. A rendszernek nincs hivatalos szabványa, mindig az tekinthető a jelenleg érvényes protokollnak, amit a legújabb hivatalos kliens használ. A programkód nyílt forráskódú, így a kis létszámú (négy-hat tagú) fejlesztőcsapat munkáját bárki segítheti javítások készítésével, amelyek a fejlesztőcsapat tagjainak jóváhagyása után kerülnek be a kliensbe.

A fejlesztőcsapat folyamatosan dolgozik a programhibák javításán és a felfedezett támadási felületek befoltozásán, ennek köszönhetően gyakorlatilag egyetlen igazán komoly incidens történt, amelynek okát és következményeit néhány órán belül sikerült orvosolni.[18]

A témába vágó hírek között gyakran lehet lopásokról és elveszett tárcafájlokról olvasni, de itt mindenképpen megjegyzendő, hogy ezek nem ez Bitcoin protokoll hibájából történnek, hanem mert a felhasználók, valamint az érintett webes szolgáltatók nem készültek fel eléggé vírus és hacker támadások ellen.

Eszteri cikkében az olvasható, hogy a lopás megakadályozása érdekében érdemes biztonsági másolatot készíteni a wallet.dat fájlról vagy tárca szolgáltatónál elhelyezni. Ez azonban csak részben igaz, ugyanis ez valóban megvéd, ha pénztárca fájl szoftver- vagy hardver-hibából eredően törlődne/megsérülne, vagy akár egy rosszindulatú támadó szándékosan törölné. Lopás esetén azonban a tolvaj nyilván átutalja érméinket egy másik címre, így hiába van biztonsági másolatunk, csak üres tárcánk képe fogad. Lopás elkerülése érdekében tehát tanácsosabb a tűzfalat pontosabban konfigurálni és a wallet.dat fájl-t titkosítani.

A rendszer biztonságos működését akadályozni szándékozó támadó egyik módszere lehet, hogy a bányászás folyamatát megakasztja és azt befolyásolja. Ehhez azonban a bányászásba fektetett számítási tudás több mint felével kell rendelkeznie, ami ismervén, hogy a bányászok által a blokkgenerálásba fektetett számítási tudás túlszárnyalja a legnagyobb szuperszámítógépek számítási kapacitását, elég valószínűtlennek tűnik.[19] A rendszer kialakítása egyébként olyan, hogy az esetleges támadónak anyagi szempontból jobban megérje a Bitcoin rendszert fenntartani, mint az ellen dolgozni.

4.3. Hardver-terhelés

A kliensprogram futás közben letölti a blokklánc hiányzó elemeit, és azokat a hash összegek újraszámolásával ellenőrzi. A teljes lánc 2012 augusztusában több, mint 195 000 blokkal 2 gigabyte méret fölött jár. Ennek letöltése, valamint a hash ellenőrzése a program első indításakor akár 8–10 órát is igénybe vehet egy középkategóriás személyi számítógépen. Saját tapasztalataim szerint a hash-számolás számításigényes volta és a folyamatos lemezhasználat miatt ez idő alatt a számítógépen minden más program érezhetően lelassult vagy teljesen használhatatlan volt. Ameddig a program nem rendelkezik a teljes blokklánccal, addig pénztárcánk aktuális egyenlegét sem láthatjuk, hiszen csak a teljes blokklánc ismeretében jelenthetjük ki, hogy tudjuk, melyik érme melyik címhez tartozik, ami igaz a sajátunkra is.

A számításigény és a blokklánc mérete elrettentő hatással lehet a potenciális új felhasználókra, a régebbi hardverrel rendelkezőket diszkriminálja, és a korlátozott erőforrásokkal bíró eszközökkel – pl. mobiltelefonnal – történő fizetés széles körű elterjedésének lehetőségét akadályozza. Ennek megoldására a nagyon közeli jövőben szükség lesz arra, hogy a protokollba beépítsék a választás lehetőségét, vagyis hogy a felhasználó dönthesse el, hogy rendelkezni akar-e a teljes blokklánccal, vagy a kisebb biztonságot nyújtó és a többi résztvevővel szemben nagyobb bizalmat igénylő, ám minimális erőforrásigénnyel rendelkező kliens-szerver jellegű architektúra mellett dönt, amelyben a blokkláncnak csak egy kis szeletét kell letölteni. Ilyen, blokklánc nélküli kliensek léteznek már, mint például a MultiBit kliens, de ezek – többek közt kevésbé biztonságos voltuk miatt – nem terjedtek el széles körben. Alternatív megoldásként lehetőség van rá, hogy valamelyik online Bitcoin szolgáltatónál (pl. piacterek, pénztárca tárhely) lévő virtuális pénztárcát használjuk, ekkor azonban a szolgáltató becsületességében és infrastrukturális felkészültségében kell megbíznunk.

5. A BITCOIN GAZDASÁGA

5.1. Piacterek

A Bitcoin értéke a belső érték nélküli pénzekre hajaz, tehát nincs nemesfémhez vagy más áruhoz kötve, valamint hiányzik a központi bank, ami a kamatok és a pénzkínálat változtatásával befolyásolhatná az árfolyamot, ezért értékét kizárólag az iránta mutatott kereslet és kínálat határozza meg. A Bitcoin gazdasága túlnyomóan a hitre épül, vagyis az értéket elsődlegesen a felhasználók száma és az ő Bitcoinba vetett hitük, bizalmuk határozza meg.

Új bitcoin-érmék bányászás útján jönnek létre, más felhasználók készletéből pedig az erre specializálódott piactereken vehetünk, ezeket váltónak vagy tőzsdének is nevezik. Napjainkban több tucat ilyen piactér üzemel, azonban ezek jelentős részén csak elenyésző mennyiségű Bitcoin folyik át, míg a kereskedési volumen több mint 70%-a az Mt.Gox nevű piactéren történik. A Bitcoin ellenértékét piacterenként különböző módszerekkel, tucatnyi valutában juttathatjuk el az eladóknak. Így fizethetünk borítékba dugott és postázott papírpénzzel, banki átutalással vagy akár online szerepjátékok saját fizetőeszközeivel (például a Second Life Linden dollárjával vagy a World of Warcraft aranyával).[20] A Bitcoin-vétel vagy -eladás a tőzsdékhez hasonló módon folyik, vagyis mindkét oldal meghatározza, hogy mennyit és milyen értékben hajlandó eladni/venni, a piactér pedig automatikusan végrehajtja a tranzakciókat amennyiben vételi ajánlati ár nagyobb vagy megegyező értékű, mint az eladási ajánlati ár. A legtöbb piactér különböző virtuális számlákon tartja nyilván a felhasználó egyenlegeit, melyekről a felhasználó kezdeményezhet utalást a rendszeren kívülre. Tehát például miután a felhasználó BTC-it euróra váltotta, ezt az euró mennyiséget tetszőleges időpontban utalhatja ki saját bankszámlájára vagy hagyhatja az Mt.Gox virtuális számláján, ami egyes jogi közegekben betétgyűjtésnek minősülhet. A különböző piacterek árai jelentősen különbözhetnek, vagyis a Bitcoin piaca nem hatékony.

A Bitcoin értéke a belső érték nélküli pénzekre hajaz, tehát nincs nemesfémhez vagy más áruhoz kötve, valamint hiányzik a központi bank, ami a kamatok és a pénzkínálat változtatásával befolyásolhatná az árfolyamot, ezért értékét kizárólag az iránta mutatott kereslet és kínálat határozza meg.

A tőzsdei jelleget elmélyítendő, egyes piacterek opciós és határidős ügyletek lebonyolítását is lehetővé teszik.

5.2. Pénzkínálat

A Bitcoin rendszer pénzkínálata előre kódolt. Jelenleg minden blokkgeneráláskor 50 BTC keletkezik a sikeres bányász jutalmaként. Ez az összeg minden 210 000 blokkonként megfeleződik, vagyis 2013-tól 25 BTC, 2017-től pedig 12.5 BTC lesz, egészen addig, amíg körülbelül 2140-ben megtörténik az utolsó blokkgenerálás, ami pénzkreálással is jár. Ekkor a rendszerben lévő összes bitcoin érme összege néhány ezreddel 21 millió alatt lesz. Az ez utáni blokkgenerálásoknál a bányász csak a tranzakciós díjakat kapja meg.

A fix pénzkínálat miatt enyhe deflációs hatás előre kódolt tényező a rendszerben. Defláció esetén a felhasználóknak érdemesebb megőrizni és gyűjtögetni a pénzüket, mint elkölteni, mert az idő múlásával egyre értékesebb lesz. Többek közt ez a tulajdonság tette népszerűvé a Bitcoint a spekulánsok körében.

Érdemes tudni, hogy a 21 millió Bitcoin mindegyike 8 decimálisig bontható, vagyis a legkisebb, tranzakcióban használható mennyiség a 0.00000001 BTC.

A fix pénzkínálat miatt enyhe deflációs hatás előre kódolt tényező a rendszerben.

5.3. Piaci résztvevők

Kik, milyen árukért és szolgáltatásokért fogadnak el Bitcoint? Igazi megkötés nincs, bárki elfogadhatja fizetőeszközként bármilyen áruért vagy szolgáltatásért.

Leggyakrabban az adományozás eszközeként láthatjuk, ezres számban beszélhetünk művészekről, non-profit szervezetekről, egyéb tartalom előállítókról, akik szívesen elfogadnak Bitcoin-adományokat.

Az online szerencsejátékok kedvelői is hamar rátaláltak a Bitcoinra, hiszen ez számos országban tiltólistás tevékenység. Az anonim pénzzel bátrabban szállnak be a játékosok egy póker, lottó vagy egyéb, a kaszinókból ismert játékba.

A Bitcoin implementálása egy már meglévő webshopba nem jelent különösebb kihívást egy programozónak. Sok üzletnek azonban a Bitcoin tranzakciók alacsony száma miatt nem éri meg erre költeni, ezért inkább ezeket a tranzakciókat egyénileg kezelik e-mail vagy egyéb kapcsolat útján. A Bitcoin wiki kereskedőket listázó oldala[21] ezres nagyságrendben tartalmaz elfogadó kereskedőket, ez azonban megtévesztő lehet, mert számos halott link és olyan szolgáltató is található, aki nem üzletszerűen végzi tevékenységét. Az elérhető kínálat nagy része jellemzően távolról végezhető vagy szorosan az online világhoz kapcsolódik, így számos webhosting, programozói, tanácsadói, nyelvoktatási, grafikai vagy ezekhez hasonló szolgáltatás érhető el. Kézzel fogható áruk széles választéka is elérhető, így fizethetünk Bitcoinnal állateledelért, kávéért, ékszerekért, ruhákért vagy autóalkatrészekért. Világszinten továbbá körülbelül két tucat szálló, hotel és étterem fogad el Bitcoint.[22]

Sokak álma, hogy minden fizetési szituációban tudjanak Bitcoint használni, ezért számos kliens támogatja a Bitcoin címekből történő QR kód generálást, amely a címek könnyebb terjesztését segíti.

1. ábra: Bitcoin címből készített QR kód

Az Android rendszerű mobiltelefonokra írt kliensprogram, a Bitcoin Wallet for Android támogatja az NFC[23] adatátvitelt, amellyel jellemzően a más mobil eszközökkel való kommunikációt, így például a Bitcoin címek átadását lehet egyszerűsíteni.

Noha ezek az újítások meggyorsíthatják a tranzakciók elindítását, de a blokkba foglalásig továbbra is legalább 10 percet kell várni, így egyelőre nehéz elképzelni, hogy tényleg így tudjunk fizetni reggel a pékségben. A blokkba foglaláson felül pedig az általánosan elfogadott szabály, hogy akkor tekinthető tényleg véglegesnek egy tranzakció, ha az azt tartalmazó blokkra már 6 másik blokk ráépült (ilyenkor a jelenleg ismert támadási/csalási módszerekkel már semmiképp nem változtatható meg a tranzakció).

5.4. Mennyit ér?

2009-es indulását követő első évben a Bitcoin egy volt az interneten felbukkanó érdekességek közül, de a rá épülő gazdaság hiányában csupán néhány tucat, a kriptográfia és az elektronikus pénzek iránt érdeklődő felhasználó bányászta és gyűjtögette. Kevesen bányászták, így az alacsony nehézségi szint miatt könnyű volt átlagos teljesítményű számítógépekkel is saját érméket generálni.

2010 februárjában hozták létre az első piacteret a Bitcoin Marketet. 1 Bitcoin ekkor néhány ezred amerikai dollárt ér.

2010 májusában történt az első olyan dokumentált tranzakció, amelyben fizikai javak cseréltek gazdát egy Bitcoin tranzakció eredményeként, amikor is a *bitcointalk.org* egy fórumfelhasználója 10 000 BTC-t utalt át egy másik felhasználónak 25 USD értékű pizzáért cserébe.[24]

2010 és 2011 nyara között a felhasználók száma és ezzel az árfolyam is fokozatosan növekedett. Egy-egy jelentősebb weblapon vagy blogban megjelent cikk után a megugrott érdeklődést az árfolyam is követte.[25]

2011 júniusában tetőzött a Bitcoin láz. A gawker Silk Road-ról szóló cikkét a világ minden részén átvették weblapok, az árfolyam emelkedése pedig spekulánsok hadát szabadította a piacterekre. Az árfolyam történelmi csúcson, 31 USD/BTC felett tetőzött, majd gyors zuhanásba kezdett. Rövid időn belül azonban több olyan esemény is történt, ami visszavetette az addigi pozitív hangulatot. Egy felhasználó napi árfolyamon 375 000 USD értékű lopást jelentett, néhány nappal később pedig a Mt.Gox-ot, a világ legnagyobb Bitcoin piacterét feltörték, többek pénzét ellopták. Az árfolyam innentől hónapokon keresztül folyamatos esést mutatott, egészen 2 USD/BTC összegig. 2012-ben újra lassú emelkedésbe kezdett az árfolyam.

5.5. Bitcoin és szabályozás

A Bitcoinica piactér volt az első olyan Bitcoinnal foglalkozó pénzügyi vállalkozás, amely regisztráltatta magát egy szabályozó testületnél (Új-Zélandon), így legálisan működtetheti Bitcoin tőzsdéjét.[26]

Az amerikai FinCEN[27] szabályzatait és a nemzetközi FATF[28] ajánlásait egyaránt a közelmúltban frissítették úgy, hogy azok az új pénzeszközökre, így a Bitcoinra is kiterjedjenek, de ezek alapján eljárás még nem indult.

2011 szeptemberében az Mt.Gox számláját zárolta franciaországi bankjuk, mivel bankszerű, betétgyűjtési tevékenységet végeztek anélkül, hogy bankként jegyezték volna be őket, amit később a Francia Központi Bank is megerősített.[29] A napvilágot látott francia nyelvű periratok szerint a per tárgya a bankszerű működés és nem a Bitcoin jogi státusza.[30]

6. ZÁRÓ GONDOLATOK

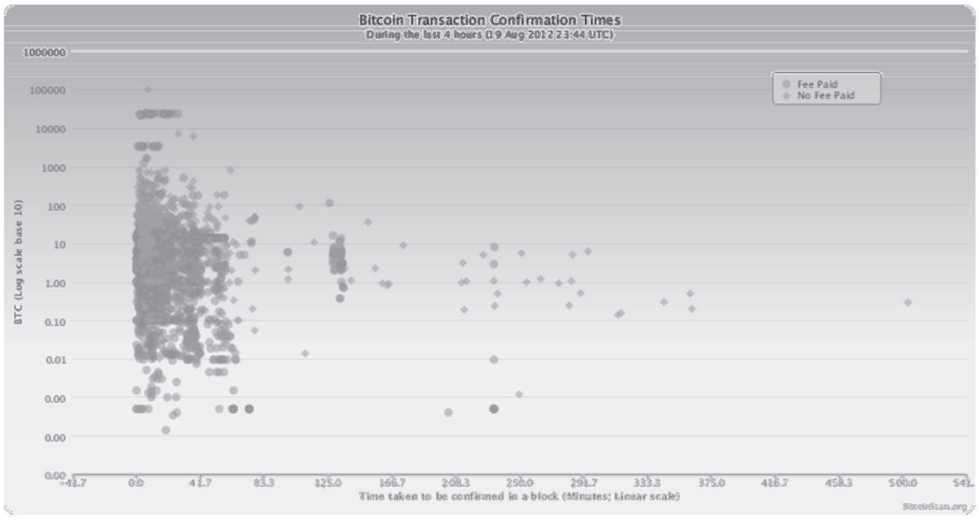
Hova tart a Bitcoin? Vajon ez lesz a jövő egyik széles körben elterjedt fizetőeszköze?

Technikai szempontból nincs ok aggodalomra. Számos Bitcoinnal kapcsolatos kutatás folyik és ezek egy része valós problémákat vet fel és javasol megoldást, mint például az a Microsoft szakemberek által készített tanulmány, ami a tranzakciós díjakat tartalmazó tranzakciók rosszindulatú eltitkolásával foglalkozik és ennek megoldására a blokkgenerálási rendszer jutalmazási módjának átalakítását javasolja[31]. Az ilyen kutatásokból leszűrt tanulságok idővel a szoftver működésének változásával járhatnak, tehát a Bitcoin rendszerre mint egy lélegző, folyamatosan fejlődő dologra kell tekintenünk.

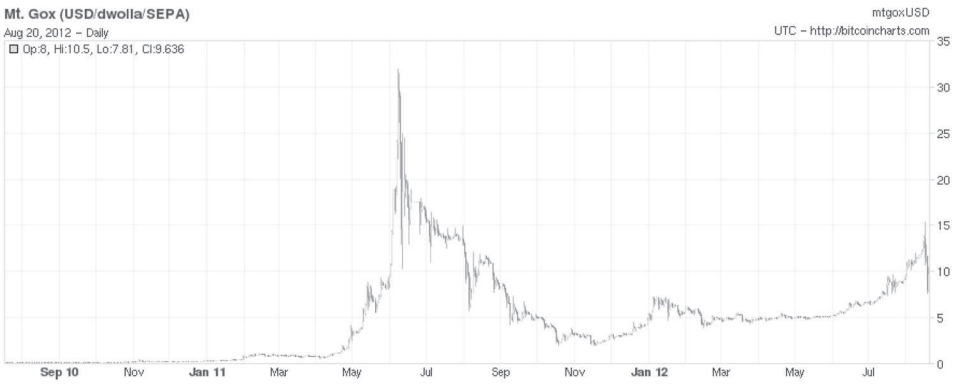
A rendszer gerincét alkotó blokklánc technológia kiemelkedően ígéretes, az említett felhasználásokon (e-pénz, domain nevek) kívül még számos más szituációban bizonyulhat használhatónak, ennek csak a programozók fantáziája szab határt.

A szabályozási kérdések tisztázatlan volta eddig sem ijesztette meg a felhasználókat, és a szabályozásnak való megfelelés talán nem is olyan fontos, mert központ híján nincs igazán jól megfogható támadási felület, ahol a rend őrei beavatkozhatnak, és ahogy azt Jon Matonis felveti, a Bitcoin a feketegazdaságban – a világ második legnagyobb gazdaságában – válhat a készpénz helyettesítőjévé és így milliárdok életének válhat mindennapi részévé.[32]

A szerzőnek van Bitcoin a birtokában.



2. ábra: Mennyi időt vesz igénybe, hogy az egyes tranzakciók blokkba kerüljenek?[33]



3. ábra: A Bitcoin dollárhoz viszonyított árfolyama az Mt.Gox piactér adatai alapján[34]

Jegyzetek

1 Eszteri Dániel: Bitcoin: Az anarchisták pénze vagy a jövő fizetőeszköze? Infokommunikáció és jog 2012/2. pp 71–79.

2 Wei Dai (1998): *b-money* http://www.weidai.com/bmoney.txt [2011. nov. 14.]

3 Nakamoto, Satoshi: *Bitcoin P2P e-cash paper* http://article.gmane.org/gmane.comp.encryption.general/12588/ [2011. nov. 15.]

4 Nakamoto, Satoshi: *Bitcoin v0.1 released* http://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html [2011. nov. 15.]

5 A blokklánc adatbázis az alábbi weboldalakon tekinthető meg kereshető és böngészhető formában. http://blockchain.info és http://blockexplorer.com/

6 A http://bitcoinstats.org/ webcímen közel valós időben követhető, hogy a menynyi ideig várakoztak a tranzakciók amíg végül blokkba foglalták őket.

7 Babaioff, M. – Dobzinski, S. – Oren, S. – Zohar, A.: *On Bitcoin and Red Balloons* http://research.microsoft.com/pubs/156072/bitcoin.pdf [2011. nov. 17.]

8 Nakamoto, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System* http://bitcoin.org/bitcoin.pdf [2011. júl. 25.]

9 Taaki, Amir: *Fat blockchain* http://bitcoinmedia.com/fat-blockchain/ [2012. febr. 4.]

10 Babaioff, M. – Dobzinski, S. – Oren, S. – Zohar, A.: *On Bitcoin and Red Balloons*

11 A Domain Name System vagyis a tartománynévrendszer gyakorlatilag az interneten használt webcímeket fordítja át a számítógép által használt protokoll számára értelmezhető formára.

12 A Namecoinra épülő DNS helyettesítő projekt weblapja: http://dot-bit.org/Main_Page

13 Greenberg, Andy: *WikiLeaks Asks For Anonymous Bitcoin Donations* http://www.forbes.com/sites/andygreenberg/2011/06/14/wikileaks-asks-for-anonymous-bitcoin-donations/ [2011. nov. 15.]

14 Chen, Adrian: The Underground Website Where You Can Buy Any Drug Imaginable http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable [2012. júl. 8.]

15 Drug Enforcement Administration – az Egyesült Államok drogügyekért felelős állami nyomozóhatósága

16 Wolf, Brett: *Senators seek crackdown on „Bitcoin" currency* http://www.reuters.com/article/2011/06/08/us-financial-bitcoins-idUSTRE7573T320110608 [2011. nov. 15.]

17 Reid, F. – Harrigan, M. (2011): *An Analysis of Anonymity in the Bitcoin System* http://arxiv.org/pdf/1107.4524v1 [2011. aug. 1.]

18 https://en.bitcoin.it/wiki/Incidents#Value_overflow

19 http://i.top500.org/sublist és http://www.bitcoinwatch.com/

20 Az összes jelentős piactér adatai elérhetők a http://bitcoincharts.com/markets/ címen.

21 A Bitcoint elfogadó kerekedőkről a https://en.bitcoin.it/wiki/Trade címen olvasható lista.

22 A Bitcoint elfogadó szállodák és éttermek a https://en.bitcoin.it/wiki/Real_world_shops címen elérhető térképen tekinthetők meg.

23 Near Field Communication: adatátviteli módszer az eszköz közvetlen közelében (jellemzően 20 centiméternél kisebb hatótáv)

24 Bitcointalk.org: *Pizza for bitcoins?* https://bitcointalk.org/index.php?topic=137.0 [2011. nov. 15.]

25 A Bitcoin történetének említésre méltó eseményeiről a https://en.bitcoin.it/wiki/History címen olvasható lista.

26 Matonis, Jon: *Bitcoinica Registers in New Zealand for Bitcoin Margin Trading* http://www.forbes.com/sites/jonmatonis/2012/04/21/bitcoinica-registers-in-new-zealand-for-bitcoin-margin-trading/ [2012. ápr. 22.]

27 Financial Crimes Enforcement Network – A pénzmosás és terrorizmus finanszírozása és egyéb pénzügyi bűncselekmények elemzésével foglalkozó Egyesült Államok-beli kormányügnökség.

28 Financial Action Task Force on Money Laundering – Nemzetközi szervezet a pénzmosás elleni küzdelem segítésére, feladata többek közt, hogy ajánlásokat fogalmazzon meg a tagországok számára.

[29] Mt.Gox Support: *All EUR transactions will be temporarily suspended within Europe, with immediate effect* https://support.mtgox.com/entries/20568322-all-eur-transactions-will-be-temporarily-suspended-within-europe-with-immediate-effect [2012. febr. 2.]

[30] Anonymus: *Bitcoin in France: first legal decision directly related to Bitcoin?* https://bitcointalk.org/index.php?PHPSESSID=df2b557f175d3d4745c26cbec3153270&topic=41317.0;all [2012. márc. 12.]

[31] Babaioff, M. – Dobzinski, S. – Oren, S. – Zohar, A.: *On Bitcoin and Red Balloons*

[32] Matonis, Jon: *Could Bitcoin Become the Currency of System D?* http://www.forbes.com/sites/jonmatonis/2012/03/19/could-bitcoin-become-the-currency-of-system-d/ [2012. ápr. 1.]

[33] Az ábra forrása a http://bitcoinstats.org/, a vízszintes tengelyen az egyes tranzakciók blokkba kerüléséig eltelt idő lineáris, függőlegesen pedig a tranzakciók összege látható logaritmikus skálán. Letöltve 2012. aug. 19-én 23:44-kor.

[34] Az ábra forrása a http://bitcoincharts.com/charts/mtgoxUSD#tgSzm1g10zm2g25, az ábra a Bitcoin amerikai dollárhoz viszonyított árfolyamát mutatja 2010 augusztusától 2012. augusztus 20-ig.