Szakdolgozat

Bitcoin hálózatok elemzése

Bakó Tamás

Biztosítási és pénzügyi matematika MSc

Kvantitatív pénzügyek szakirány

Eötvös Loránd Tudományegyetem
Természettudományi Kar

Budapesti Corvinus Egyetem
Közgazdaságtudományi Kar

Témavezetők:

Dr. Csabai István

egyetemi tanár

Komplex Rendszerek Fizikája Tanszék

Dr. Berlinger Edina

egyetemi docens

Befektetések és Vállalati Pénzügy Tanszék

Budapest, 2015

Köszönetnyilvánítás

Nagy hálával tartozom témavezetőimnek dr. Berlinger Edinának és dr. Csabai Istvánnak velem és értem végzett munkájukért, türelmükért. Kiemelt köszönettel tartozom továbbá Kondor Dánielnek önzetlen, nagylelkű, munkámat komoly mértékben segítő közreműködéséért.

Illesse köszönet Badics Milánt, Czimbalmos Gábort, Kondor Imrét, Palla Gergelyt, Papp Gábort, Pollner Pétert, Pósfai Mártont, Sándor Máté Csabát, Sebők Tamást, Stéger Józsefet, Szabó Dávidot, kutatócsoportunk tagjait, akiknek segítsége nélkül ez a munka nem jöhetett volna létre.

Tartalomjegyzék

Bevezetés

A XXI. század információs technológiai fejlettsége az életünk minden területén nagy változásokat okozott. Az internet és a számítógépes hálózatok ilyen mértékű elterjedése alapvető globális változásokat idézett elő mind a kommunikáció sebességében és eszközeiben, mind az ipari és társadalmi rendszerekben. Ez alól természetesen nem maradt ki a gazdasági/ pénzügyi szektor sem. A 2007/2008-as válságot követően megjelentek olyan különleges pénzügyi instrumentumok, amelyek - bár nem feltétlen felelnek meg a klasszikus közgazdaságtani pénzfogalomnak - mégis nagy népszerűségre tettek szert. Ez a dolgozat a legnagyobb visszhangot előidéző és nagy megosztást kiváltó digitális fizetőeszközzel, (cryptocurrency) a bitcoinnal foglalkozik.

A dolgozatot két nagy egységre bontom. Az első részében (I-IV fejezet) áttekintem a cryptocurrency fogalmát, a mélyebb megértés érdekében kitérve a technikai és matematikai/informatikai alapjaira is. Ezen kívül összefoglalom és elemezem a bitcoin fogadtatását a világban, az indulásának körülményeit és érzékelhető hatását. A második részben összefoglalom és értelmezem azokat az eredményeket, amelyeket az ELTE és Corvinus egyetem közös kutatócsoportjában végeztünk (V-IX. fejezet). Vizsgálódásunk előnye és hátránya is egyben a bitcoin hálózat egyedülállósága, amelynek különlegessége az ingyenesen hozzáférhető publikus pénzügyi adatok mennyisége, amely más pénzügyi rendszerekben sehol nem állt volna rendelkezésünkre. A hátrány szintén ebből származik. Ilyen mennyiségű adat tárolásához és vizsgálatához komoly erőforrásokat kellett igénybe vennünk az ELTE-n.

Ezen kutatásba való bekapcsolódásom lehetővé tette, hogy belelássak nagy adatbázisok kezelésének nehézségeibe, valamint a matematikai, fizikai, informatikai és közgazdaságtani ismereteim komplex alkalmazásába. Még ha nem is valószínű, hogy a bitcoin, vagy egy hozzá hasonló rendszer hamarosan átalakítaná a teljes globális pénzügyi piacot, de fontos komolyan venni, mert elveiben olyan ötleteket és újításokat tartalmaz, amelyet adaptálni lehet számos területre.

A dolgozat a teljesség igénye nélkül, de a lehető legszélesebb spektrumot felölelve szeretné körüljárni a témát, ami egy ilyen friss témánál nem volt könnyű, mert erősen interdiszciplináris környezetet igényelt. Nagyon szerencsésnek érzem magam, mert egy olyan kiváló kutatócsoport tagja lehettem, amely tevékenysége átívelt a matematika, fizika, közgazdaságtan, és informatika tudományterületek mindegyikén.

I. Fejezet

A bitcoin elméleti alapjai [1]

1. A bitcoin születése

A bitcoin alapjait egy 2008 októberében megjelent cikk fektette le, melyet Satoshi Nakamoto álnév alatt töltöttek föl a világhálóra. Ennek a cikknek a célja az volt, hogy megmutassa, hogyan lehet egy olyan elektronikus fizetőeszközt technikailag megalkotni, amely gyors és biztonságos pénzügyi tranzakciókat tesz lehetővé közvetlenül, tehát semmilyen pénzügyi közvetítő nem szükséges hozzá.

Azért érezték szükségesnek egy alapvetően új rendszer kidolgozását, mert a cikk állítása szerint, a pénzügyi tranzakciók költségesek, és a harmadik fél bizalmán alapulnak. Ezért a pénzügyi közvetítők a visszaélések és csalások elkerülése végett több információt gyűjtenek be az ügyfelekről, mint amennyire szükségük lenne a tranzakciók lebonyolítása érdekében, emellett gyakran korlátozzák a minimális tranzakciók méretét, gyakoriságát. Ezen információk feldolgozása, tárolása tovább növeli a tranzakciók költségét.

A cikk szerzői a megoldást egy olyan rendszer kidolgozásában látják, amely nem a közvetítőbe helyezett bizalomra épít, hanem kriptográfiára és elemi számítások sokaságára bízza a tranzakciók validálását, egy peer-to-peer hálózaton. Ez mindaddig biztonságot nyújt az egész rendszernek, amíg a rendszert becsületesen használni kívánók összessége több számítási kapacitással bír, mint bármely a rendszer kijátszására apelláló személy vagy csoport a hálózatban.

2. Peer-to-peer hálózatok [2]

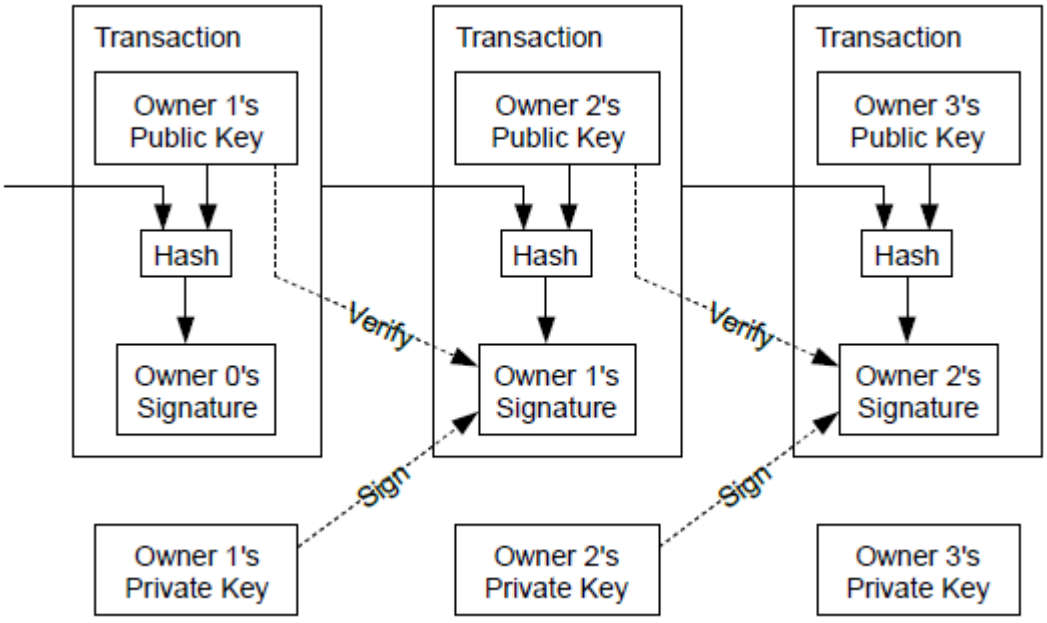
A peer-to-peer (P2P) hálózatok az egyenrangú résztvevők együttműködésén alapuló rendszerek. A hálózat lényege, hogy azok végpontjai közvetlenül egymással kommunikálnak, központi kitüntetett csomópont (szerver) nélkül. A P2P hálózatok a kliens-szerver kapcsolathoz képest jelentősen eltérő módon működnek: a szerepek nincsenek előre meghatározva; többnyire követelmény is, hogy az összes résztvevő képes legyen valamilyen erőforrást a rendszer egésze számára elérhetővé tenni viszonzásképp az általa igénybevett szolgáltatásokért. Ezek többnyire szimultán működnek, tehát az egyes csomópontok egyszerre töltik be bizonyos résztvevők felé a szerver, bizonyos más résztvevők felé a kliens szerepet. Szomszédsági alapon működő hálózatok ezek: amellett, hogy nincs szükség benne

kitüntetett szereplőre, a rendszer úgy is nagymértékű stabilitást mutat, hogy minden csomópont csak korlátos számú másik csomóponttal tart fenn kapcsolatot. Ez a működési mód igazából nem újdonság: az „ős- Internet” pontosan ugyanígy működött.

3. A bitcoin tranzakciók elve

Az elektronikus fizetőeszköz alapegységét úgy definiálták, mint egy digitális aláírásokból vett láncot, sorozatot. Minden tulajdonos úgy küldi át az egységét egy másiknak, hogy ellátja a saját digitális aláírásával az előző tranzakcióról (hasítóérték), és a következő tulajdonos publikus kulcsával. Ezután minden új tulajdonos azonosíthatja magát a privát kulcsával, hogy övé a pénz.

Tranzakciók felépítése



1. ábra
A tranzakciók sematikus felépítése: a digitális aláírás hitelesíti a pénzcserét

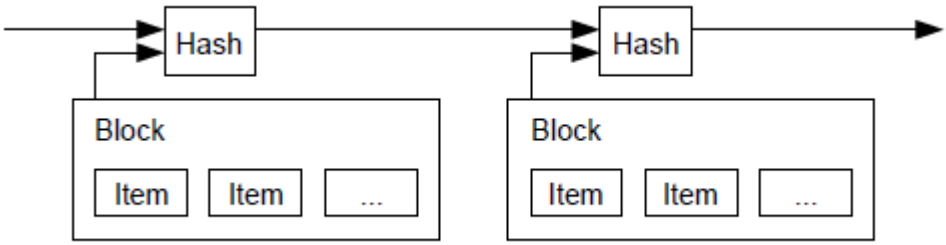
Ez biztosítja, hogy jó fél kapja meg a pénzt. Egy probléma még nincs megoldva, mégpedig az, hogy az új tulajdonos nem tudja ellenőrizni, hogy esetleg nem lett-e már kétszer elutalva ugyanaz a pénz. Ennek egyszerű megoldása lenne egy központi ellenőrző szerver, de ez ismét támadási felületet nyújtana, amelyet pont elkerülni szeretnének egy ilyen modellű fizetőeszköz tervezésekor. A legkézenfekvőbb és egyben legbiztosabb megoldás, hogy az új tulajdonos meggyőződhessen róla, hogy csak és kizárólag ő birtokolja a kapott pénzt, ha

hozzáférése van a rendszerben történt összes tranzakcióhoz. Ezt egy olyan modell keretében érdemes létrehozni, ahol az a tranzakció tekinthető érvényesnek, ami időben először történt. Tehát egy olyan adatstruktúra megalkotására van szükség, amely nyilvános minden résztvevő számára és egy pontos időrendiséget biztosít, azaz a hálózatban található összes szereplő döntő többsége megegyezik egy azonos időrendiségben. Ez a módszer egy sokszereplős piacon nagy biztonságot fog jelenteni, mert közel lehetetlen egy alternatív többséget megszerezni, ha minden szereplőnek rendelkezésére áll ugyanaz a tranzakciós lista.

4. Timestamp rendszer és proof of work [3]

Ennek a problémának a megoldáshoz szükség van egy hash[1] (továbbiakban hasítóérték) blokk rendszer létrehozására, ahol a blokkokat ellátjuk egy időbélyeggel (timestamp) , amely biztosítja, hogy az adott blokkban tárolt elemek megtörténtek az adott időbélyeg időpontjáig. Minden időbélyeg tartalmazza az előző időbélyeg időpontját is. Ezzel egy láncot hozunk létre, mely újabb tagjait az előző tag megléte hitelesíti.

Blokklánc elvi felépítése



2. ábra

A blokklánc időrendiségének elvi felépítése: az időrendiséget az egyedi időbélyegek biztosítják

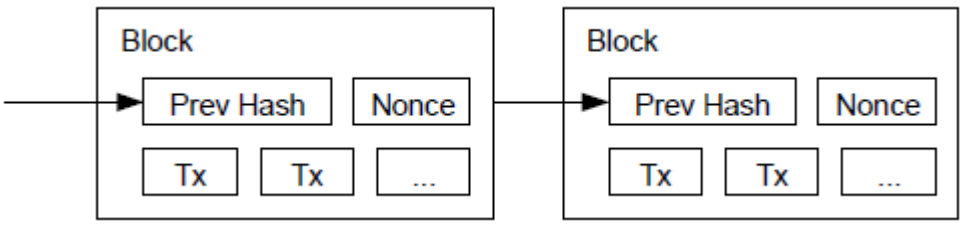
Ennek az időbélyegző rendszernek kell tehát peer-to-peer alapon működnie. A technikai megoldáshoz a proof-of-work modell alkalmazható a biztonság biztosítására.

A proof-of-work egy olyan számítástechnikai validáló rendszer, amelyben bármilyen művelet végrehajtásának feltétele valamilyen számítás igényes feladat elvégezése. Ez akkor működik hatékonyan, ha egy bizonyos aszimmetriát követ. A feladat kellően nehéz, hogy akárki ne akarja megpróbálni (alapvetően a spamek megfékezésére fejlesztették ki) és emellett könnyen ellenőrizhető, hogy valóban sikerült a feladatot megoldani (automatikusan engedélyezze az adott tevékenységet). A proof to work sémák többsége úgy működik, hogy

[1] A hash függvények magyarul hasítófüggvények olyan számítástechnikában használt algoritmusok, amelyekkel bármilyen hosszúságú adatot adott hosszúságra képezhetünk le. Az így kapott véges adatot hash vagy hasítóértéknek szokás nevezni. Ezek az algoritmusok az elektronikus aláírás kulcsfontosságú elemei.

egy bizonyos hasítófügvénnyel generálják a hasítóértékeket mindaddig, amíg egy kritériumnak meg nem felel az értékük. A hasítófüggvény bármely bemeneti bitjének megváltozásával véletlen módon változik meg a hasítóérték. A bitcoin rendszerben úgynevezett SHA-256-os hasítófüggvényt használnak [4]. Minden blokkhoz társítanak egy nonce[2]-t és a hálózat szereplői megpróbálhatják megtalálni a blokk megfelelő hasítóértékét. A hasítóérték elején található zéró elemek számával lehet szabályozni a probléma megoldásához szükséges számítástechnikai kapacitást: ez az a kritérium, amit a hasítóértéknek teljesítenie kell. Például, ha ilyen 256 bit hosszú hasítófüggvényt használunk, akkor 2^{256} féle hasítóértéket kaphatunk, de ha 20 nullával kezdődőt keresünk, akkor csak 2^{236} a számunkra elfogadható. Így a valószínűség, hogy eltalálják nagyon kicsi lesz. Jelen pillanatban egy egyszeri próbálkozás sikerességének valószínűsége: $4.89\ 10^{-21}$. Ha valakinek ez sikerült, akkor az adott blokkot felülírni nem lehetséges, csak akkor, ha egy hasonló nehézségű problémát újra megoldanak. Ennek az elkerülése a blokkok láncba helyezésével biztosítható. Tehát bármely múltbéli blokk megváltoztatásához szükséges az összes olyan blokk problémáját megoldani, ami a jelen és a megváltoztatni kívánt múltbéli blokk között van.

Blokklánc felépítése



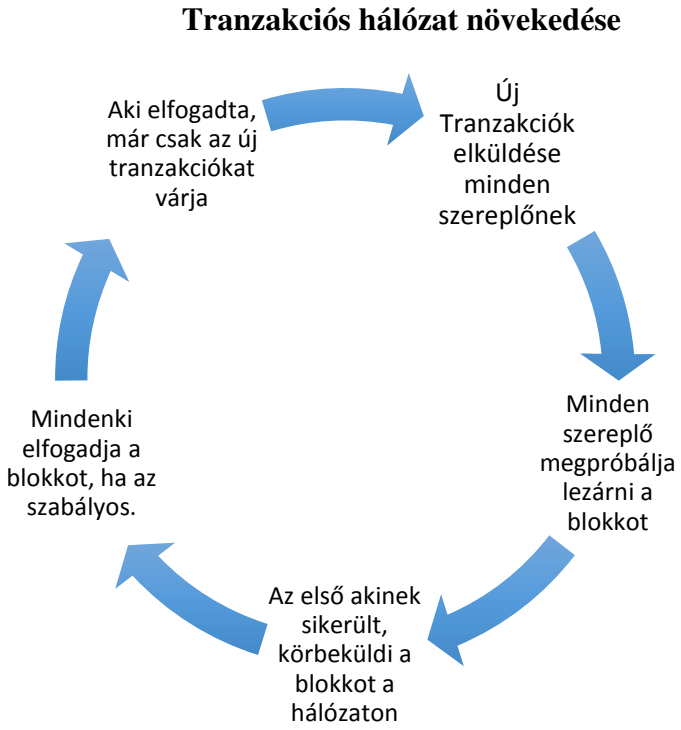
3. ábra
Proof to work sémájú blokklánc felépítése: a múltat csak az összes blokk proof to work problémájának megoldásával lehet felülírni

Ha a rendszerünk gyakori időközönként készít blokkokat, akkor ezzel nagy stabilitást érhetünk el, hiszen minél hosszabb a lánc - amiben a többség megegyezik -, annál dominánsabban szorítja ki az összes olyan próbálkozást, amely újra tervezi írni a múltat. Annak érdekében, hogy a blokkok létrejöttének megfelelő ütemét biztosítsák, a proof-of-work nehézségét egy mozgóátlag számítás biztosítja, amely egy fix általagos *létrejövő blokkok száma/óra* érteket tart.

[2] A nonce a kriptográfiában egy tetszőleges szám, amit egyetlen egyszer használnak fel.

5. A hálózat működési elve

Ahhoz, hogy egy ilyen rendszer pénzügyi tranzakciókat tudjon közvetíteni, a következő módon kell felépíteni a hálózatot. Minden hálózatban szereplő megkapja az új tranzakciókat. Minden szereplő blokkba rendezi az új tranzakciókat és megpróbálja a dinamikusan növekvő blokkhoz megoldani a proof-of-work problémát. Az a szereplő, akinek ez először sikerül a blokkját körbeküldi mindenkinek, mint a blokklánc (blockchain) egy újabb elemét. A szereplők csak akkor fogadják el ezt a blokkot, ha a benne található összes tranzakciónak csak egy múltja van. Ha ez teljesül, akkor az összes szereplő azzal tanúsítja az elfogadást, hogy ezen blokkra építve kezd neki az újabb tranzakciók blokkba helyezéséhez és a folyamat kezdődik előről.



4. ábra
A tranzakciós hitelesítés lépései

Ennek a hálózatnak a stabilitása meglehetősen nagy, hiszen nem szükséges minden szereplőnek azonnal reagálnia, sem részt vennie az adatátvételben, sem a blokkosítás folyamatában. A késve érkezett szereplők abban a pillanatban tudni fogják, hogy hány blokkal vannak lemaradva, ahogy megkapják a legújabbat. Az egész rendszert a leghosszabb

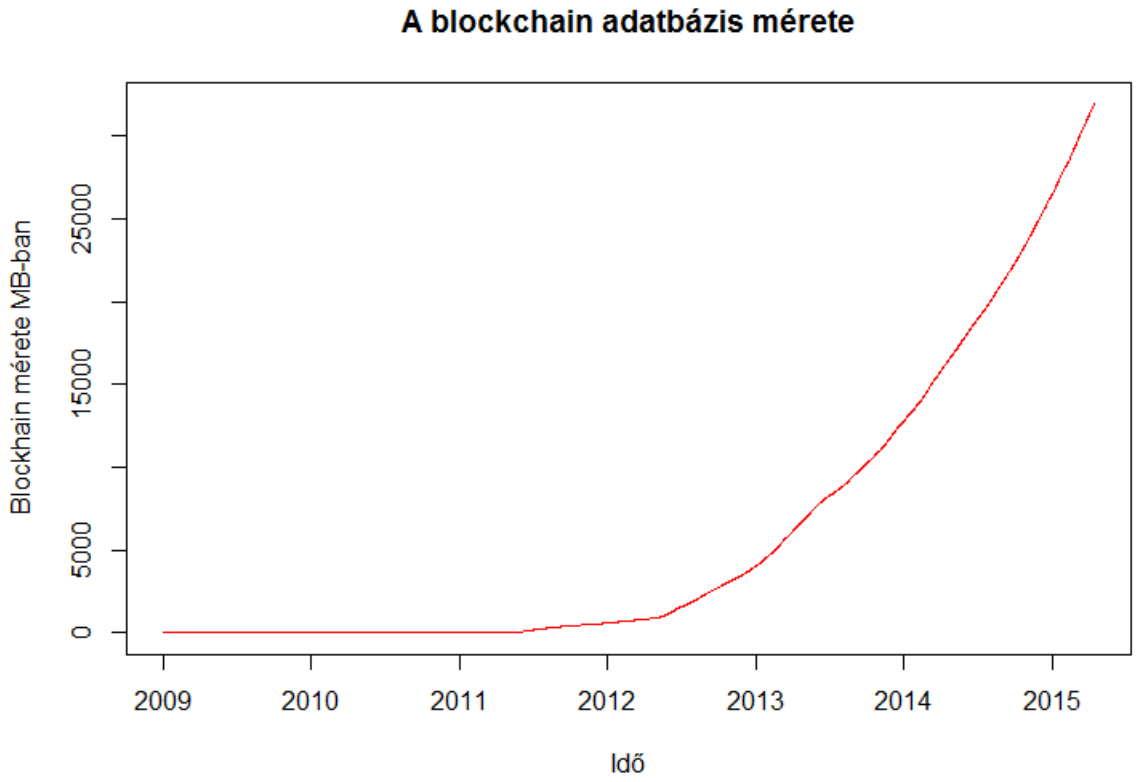
blokklánc fogja vezérelni, ami ha kellő számú szereplőnél megtalálható, akkor a rendszer nagy dinamikai változásokat képes elviselni.

6. Motiváció, tranzakciók részletei

Mint láthattuk, egy ilyen rendszer több lépcsőben garantálja a pénz valódiságát és a tranzakció hitelességét. Mivel az egész rendszer szereplőinek teljesítmény (számítási kapacitása) igénye azoknál összpontosul, akik validáláshoz szükséges blokkok proof-to-work problémáját oldják meg, szükség van ezen felhasználók motivációjára. Ez egy nagyon jó lehetőség arra, hogy az egész rendszerben található pénzmennyiséget is szabályozni lehessen. Minden blokk első tranzakcióját ezért úgy választják meg, hogy egy olyan fix összegű tranzakció legyen, aminek nincs bemeneti oldala, kimeneti oldalát a proof-of-work problémát megoldó (továbbiakban bányász) határozhatja meg. Ezzel a rendszerben található összes pénz mennyisége növekedett, így a bányászoknak is megéri a blokkosítást elvégezni és a rendszer is dinamikusan növekszik. A motivációt a hálózaton másképp is meg lehet oldani, ha az összes blokkban lévő tranzakcióhoz tranzakciós költséget rendelünk. Ez a lehetőség a hálózat növekedésével szétoszthatja a terhet a tranzakciós partnerek között, de a két módszer kombinálása is lehetséges. Ez emlékeztethet minket egy hagyományos pénzügyi közvetítő rendszerére, de a bizalom igényt kiküszöböli, mert minden bányásznak az érdeke egy hiteles blokk létrehozása (csak ekkora kapja meg a jutalékát) és a proof-to-work probléma nehézségének ésszerű kalibrálása mellett az összes pénzmennyiség növekedése független a bányászok számától és a bevitt teljesítménytől.

Egy másik problémát is megold ez a dinamikus szabályozhatóság, mégpedig a bányászok fizikai energia szükségletének költségét. Ez alatt a probléma alatt azt értem, hogy addig fog egy bányász nagy teljesítményű számítási kapacitást rászánni egy probléma számítására, amíg az azért kapott pénzből tudja fedezni a saját fenntartási költségeit. A szakdolgozat készülésének idején jutottak a bányászok arra a pontra, ahol az önszabályozás életbe lépett. Egyes bányászok kiszállnak, ezzel a probléma is egyszerűsödni fog. [5]

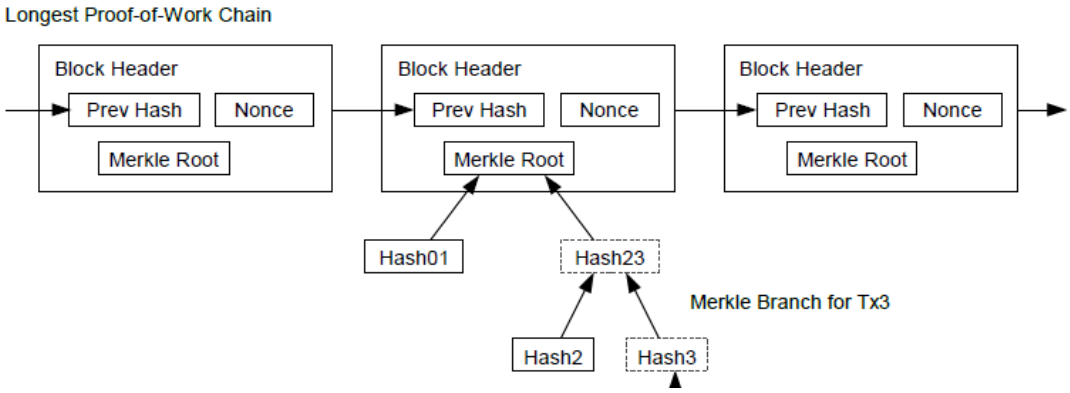
Aggodalomra adhat még okot a hálózat és a tranzakciók számának növekedésével a teljes adatbázis méretállománya. Ezt bár alulbecsülték 2008-ban az állomány növekedése az egységnyi adattárolás költségéhez képest kisebb ütemben növekszik, tehát technikai problémákba nem fog ütközni egy ilyen rendszer életben tartása a közeljövőben.



5. ábra
A bitcoin blokklánc méretének változása a kezdetektől napjainkig

Már erre utaltam, de érdemes jobban megvizsgálni, hogy nem szükséges egy szereplőnek minden hálózati információról tudnia ahhoz, hogy egy biztonságos és hiteles tranzakciót hajtson végre. Elég a blokk fejléceiből álló leghosszabb láncot ismernie (az elfogadott blokklánc fejléceit) , amely a következőképpen épül föl:

Blokk fejléceiből álló lánc szerkezete



***6**. ábra*
A tranzakciós múlt tömörítésének elve: egy biztonságos tranzakcióhoz elegendő ismerni a fejlécekből álló leghosszabb láncot

A fejléc tartalmazza az egyes tranzakciók hasító értékeiből álló Merkle fát. Ez tulajdonképp egy hozzárendelés, hogy az adott tranzakció melyik időbélyegű blokkban helyezkedik el. Így az adott szereplő bármely tranzakcióról megbizonyosodhat, hogy a hálózat elfogadta-e anélkül, hogy a konkrét tranzakciós múltat végignézné.

7. A hálózat stabilitása

Elméleti kérdés lehet, hogy mégis milyen biztonságos egy ilyen rendszer. Ehhez vizsgáljunk meg egy egyszerű példát arra vonatkozólag, hogy mi történne, ha egy támadó gyorsabban akarna egy hosszabb alternatív múltú láncot létrehozni, mint a becsületes bányászok azért, hogy saját előnyre tegyen szert. Erre tekinthetnénk akár úgy, mint a virtuális pénzhamisításra, de fontos egy ilyen stressz tesztnél végiggondolni, hogy ez milyen következményekkel járhat. Egy ilyen fajta támadás nem változtatná meg a rendszer struktúráját, az egyes szereplők nem fogadhatnának el hamis utalásokat, nem tudna a támadó új pénzt teremteni a rendszerben. Maximum a tranzakciós múltat tudná megváltozatni, ami számára csak akkor jelent értéket, ha a saját tranzakcióját tudja meg nem történtté tenni: „visszalopni” a már elutalt pénzét.

Ezt, a becsületes bányász és a támadó versenyét egy binomiális véletlen bolyongással lehet modellezni. Ahol +1 a lépés,ha a becsületes bányásznak sikerül növelnie a blokkláncot, és -1 ha a különbség közöttük eggyel csökken, mert a támadónak sikerül a saját láncát növelnie. Annak a valószínűsége, hogy egy bizonyos hátrányt egy támadó ledolgoz analóg a Gambler's ruin problémával.

Gambler's ruin [6] problémát sokféleképpen szokás megfogalmazni egyik megfogalmazás, hogy ha egy szerencsejátékos véges összeggel játszik egy 0 várható értékű játékot, akkor egy végtelen tőkéjű bankkal szemben veszteni fog. Számunkra jobb megfogalmazása a problémának egy szerencsejátékos, akinek végtelen mennyiségű hitel áll rendelkezésére és egy fix adósságot próbál visszanyerni. Legyen p annak a valószínűsége, hogy a becsületes bányásznak sikerül növelnie egy új blokkal a blokkláncot. Legyen q , hogy a támadónak sikerül. Legyen q_z pedig annak a valószínűsége, hogy a támadó megelőzi a z-vel hosszabb blokklánc hosszát, így a támadás sikeres.

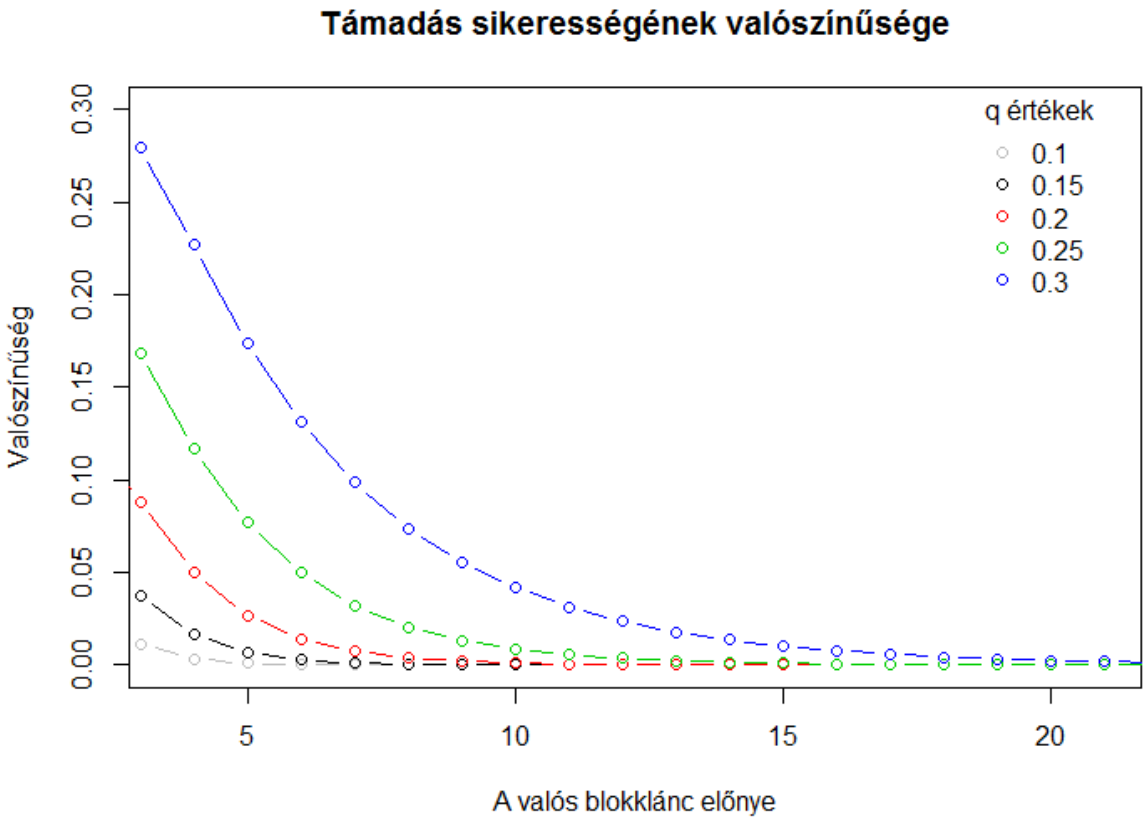
$$q_z = \begin{cases} 1 \; ha \; p \leq q \\ (q/p)^z \; ha \; p > q \end{cases}$$

Mint láthatjuk, ha p > q akkor a valószínűség exponenciálisan nő, ahogy a blokk távolság nő. Egy valós pénzszerzési támadást úgy képzelhetünk el, hogy a támadó fél küld egy bizonyos összeget a fogadó félnek és abban a pillanatban, ahogy a küldés megtörtént megpróbál egy alternatív láncot készíteni, hogy az utalást semmissé tegye. Ekkor egy sikeres csalás Poisson eloszlással modellezhető.

$$\lambda = z\frac{q}{p}$$

Ahol z itt a tranzakció megtörténte óta megfejtett új becsületes blokkok száma. A valószínűség a következőképpen számolható ki:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}\left(1 - \left(\frac{q}{p}\right)^{(z-k)}\right)$$



7. ábra

Szimulált támadás sikerességének valószínűsége a becsületes lánctulajdonosok előnyének függvényében

A fenti ábrán látható különböző q valószínűségek mellett a támadás sikerességének valószínűsége a becsületes bányászok előnyének függvényében. Ez alapján bátran mondhatjuk, hogy egy támadónak nagyon nehéz dolga van, ha egy sokszereplős becsületes bányász hálózatban próbál csalni.

II. Fejezet

A bitcoin

1.A bitcoin debütálása [7]

A 2008. október 31- én nyilvánosságra hozott cikk után nem sokkal, a cikk mögött álló egyén vagy egyének, felraktak az internetre egy nyílt forráskódú szoftvert, amely a tárgyalt modell alapján működik. Ennek első blokkja 2009. január 3 - án 18:15:05-kor generálódott és még a különleges új pénzt teremtő tranzakción kívül mást nem tartalmazott. A szoftvert 2009. január 9 - én hozták nyilvánosságra.

Block 0 [8]

- Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
- Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
- Time: 2009-01-03 18:15:05
- Difficulty: 1 ("Bits": 1d00ffff)
- Transactions: 1
- Total BTC: 50
- Size: 285 bytes
- Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
- Nonce: 2083236893
- Raw block

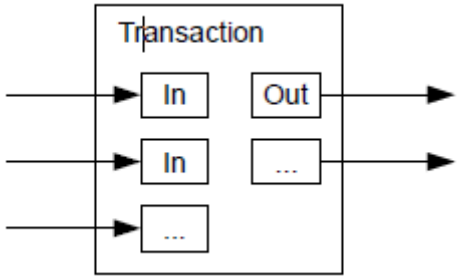
Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

Az első két számlatulajdonos közötti pénz tranzakció három napra rá történt, a 170. blokkban. Fontos megvizsgálnunk az adatok későbbi elemzéséhez, hogy hogyan is épül fel egy tranzakció. Alapvetően a rendszer lehetővé tenné, hogy minden apró összeget külön tranzakcióban könyveljünk el, de ennél komplexebb módon oldották meg az utalásokat. Minden tranzakció több bemenettel és több kimenettel rendelkezik. Technikailag úgy néz ki egy átlagos tranzakció, hogy a tranzakció bemenetén lesznek azok az előzmény tranzakció kimenetek, amikből az utaló fél szeretné a pénzét tovább utalni (tehát rendelkezik azoknak a számláknak a privát kulcsával). A kimenetén pedig szerepelni fog a célszámla címe, valamint a bemenetek

összértékének többlete a célösszeghez képest, ami az utaló fél egy számlájára visszamutat (erre gondolhatunk úgy, mint a visszajáró elfogadására).

Tranzakció felépítése



8. ábra
Egy átlagos tranzakció: több bemenet és kimenet található benne

2. Bitcoin anonimitása

A bitcoin hálózat fontos tulajdonsága, hogy mind a tranzakciók, mind a számlák abszolút egyediek: különböző privát kulcs és cím jellemzi őket, de semmilyen más azonosításra nincs szükség. Ezért egy informatikában kicsit is jártas személynek elég könnyű szinte teljesen anonimnak maradnia a hálózaton. Ezt segíti, hogy egy személy (ip cím, a hálózat bármilyen emberi vagy gép szereplője) akármennyi számlacímmel rendelkezhet: akár minden utaláshoz használhat új címet. A bitcoin ezen tulajdonsága természetesen kedvezett a „Deep webnek". Ha egy rendszer természetéből adódóan védi a felhasználóit, akkor könnyű piszkos ügyletekre használni. Ez a felhasználó – szabadság - majd később látni fogjuk -, hogy igencsak megnehezíti a hálózat elemzését.

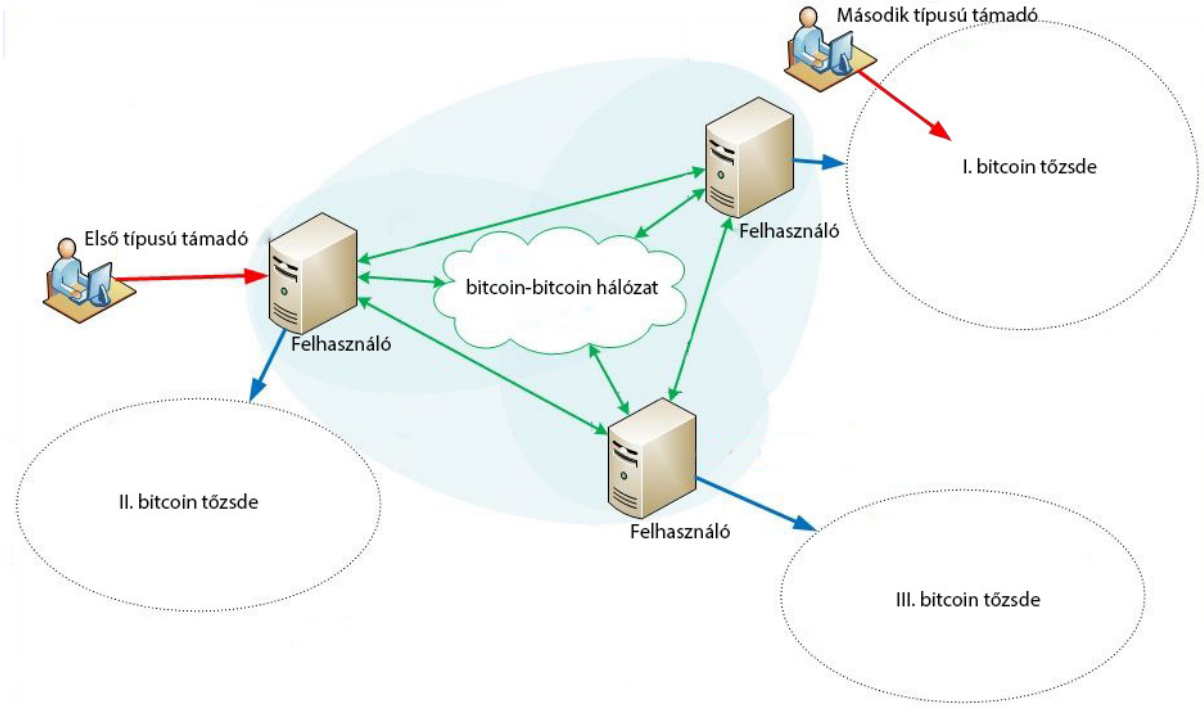
3.Bitcoin visszaélések

A bitcoin főként a vele kapcsolatos botrányok miatt kapott nagy médiavisszhangot. Ezért fontos megvizsgálni, hogy a sikeres bitcoin visszaélések, támadások milyen jellegűek voltak és mik a közös tulajdonságaik. Ezen visszaéléseket három nagy csoportba sorolhatjuk. Az egyik a privát kulcs megszerzésére irányuló támadások. Mivel ez az egyetlen egy módja bármely számlán történő utalásnak, ezért ezt próbálják megszerezni a támadók. Erre egy tapasztalt hackernek vagy hackercsoportnak azért van esélye, mert a privát kulcsot a számítógép tárolja. Nem a felhasználó üti be, hanem valamilyen felhasználófiókja tárolja, amit egy sokkal rövidebb jelszóval véd a számlatulajdonos, és ezt a jelszót szerzik meg valamilyen módon a támadók. Ezek a támadások azért gyakoriak, mert az átlag informatikai felhasználók nagyon gyenge jelszavakat használnak, amiket sokszor találgatva is véges időn belül meg lehet fejteni. Az ilyen

típusú visszaélésre a legjobb analógia a hagyományos rablás, mivel a rablók teljesen a rendszer szabályai szerint utalják tovább maguknak a teljesen valós pénzt és az anonimitást kihasználva elég gyorsan keresztülmossák a zsákmányolt pénzt a rendszeren.

A másik típusa a csalásoknak az árfolyam és a kereskedés manipulálása. Az egész bitcoin rendszer stabilitása és magas fokú védelme a bitcoin-bitcoin tranzakciókra vonatkozik és nem a devizapiacokra. A devizapiaci tranzakciók nem is jelennek meg a hálózaton. Ezek legtöbbje olyan interneten működő ajánlat- vezérelt piac, amelyek nyilvános ajánlati könyvvel, saját belső adatbázissal és ismeretlen számú belső bitcoin számlával rendelkeznek. A hackerek itt ezt a belső adatbázist törik fel, vagy valamilyen módon módosítják, így manipulálva áttételesen az árfolyamot, amelyet különböző ügyletekkel kihasználnak akár egy, akár több piacon. Sok esetben sajnos, mivel a tőzsdék üzemeltetőit sem ismerjük, nem lehet különválasztani a tőzsdéken történt támadásokat és az ezzel a kijelentéssel leplezett belső sikkasztásokat.

Lehetséges visszaélések típusai



9. ábra

A bitcoin tranzakciós hálózat nem véd a klasszikus hackertámadások sem a zárt számlavezetésű tőzsdék támadása ellen

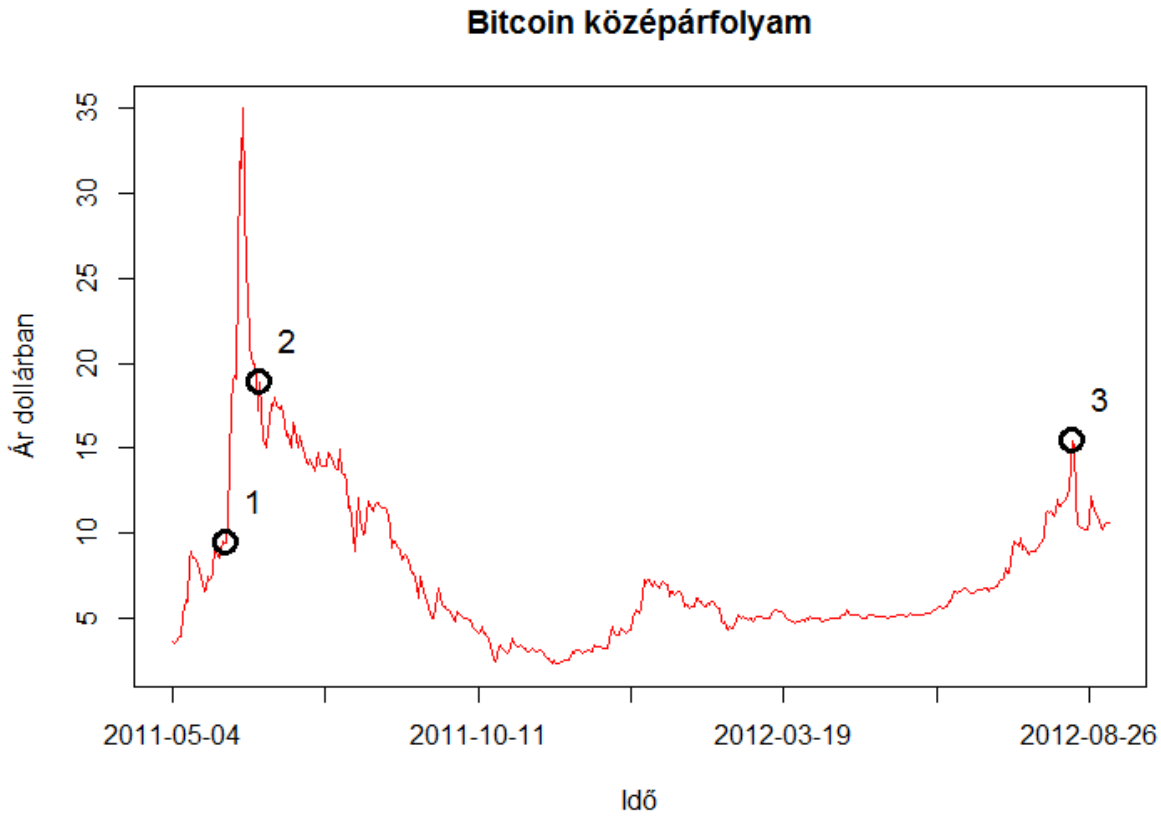
A harmadik típus a nem informatikai vagy digitális ügyeskedéshez köthető visszaélés. Ide sorolható az összes klasszikus csalás, amely minden pénzügyi területen ismerős: piramis játékok (Ponzi séma) , bizalom alapú visszaélések, nem teljesített tranzakciók és így tovább.

Mindhárom fent tárgyalt típusban közös, hogy gyakran emberi mulasztáson alapulnak, és sosem a hálózatot támadják, hanem a peremeken lévő kiskapukat használják ki. Az érdekessége ezeknek, hogy egy visszaélést nagyon nehezen lehet semmissé tenni. Ennek oka pont a bitcoin hálózat nagyon erős védelme: a lopott, de valós pénzek továbbutalását a rendszer éppúgy védi, mint a tiszta forrásból származókat. Olyan mértékű számítógép kapacitás mellett, amely a jelenben generálja a blokkokat, a gyakorlatban szinte nem lehet akkora a csalás értéke, amelynél megérné - vagy egyáltalán kivitelezhetővé válna - az utalások utólagos manipulálása. Ez, bár itt nem egyértelműen ilyen kontextusban látjuk, de ha végiggondoljuk, akkor ez azt jelenti, hogy a hálózati elv kiválóan működik.

4. Bitcoin felemelkedése [9]

A bitcoin hálózatra 2009 és 2010 között tulajdonképpen, mint egy kísérletre lehet tekinteni. A fordulatot – de még nem a népszerűséget - az első BTCUSD piac megjelenése jelentette 2010 februárjában. Ekkor nagyságrendileg 1300 BTC-t lehetett vásárolni 1 USA dollárért. Ez az év az azóta híressé vált piacok megjelenését, a bányászat fellendülését, a proof-to-work nehézség drasztikus emelkedését hozta. Az év végére a bitcoin középárfolyama el-elérte az 1 dollárt.

2011 és 2013 között a bitcoin piac folyamatosan nőtt, az árfolyam szépen lassan emelkedett, megjelentek olyan közszereplők, nagy entitások, akik támogatták a kezdeményezést, elfogadtak bitcoint. Bár a népszerűséget vagy inkább hírhedtséget a körülötte kialakult botrányok hozták meg. A teljesség igénye nélkül szeretnék felsorolni néhány nagy port kavart eseményt és annak tükröződését az árfolyamon. Mindezt annak érdekében, hogy ha közgazdasági szempontból tekintünk a bitcoinra, ismerjük meg a különböző történéseket.



10. ábra

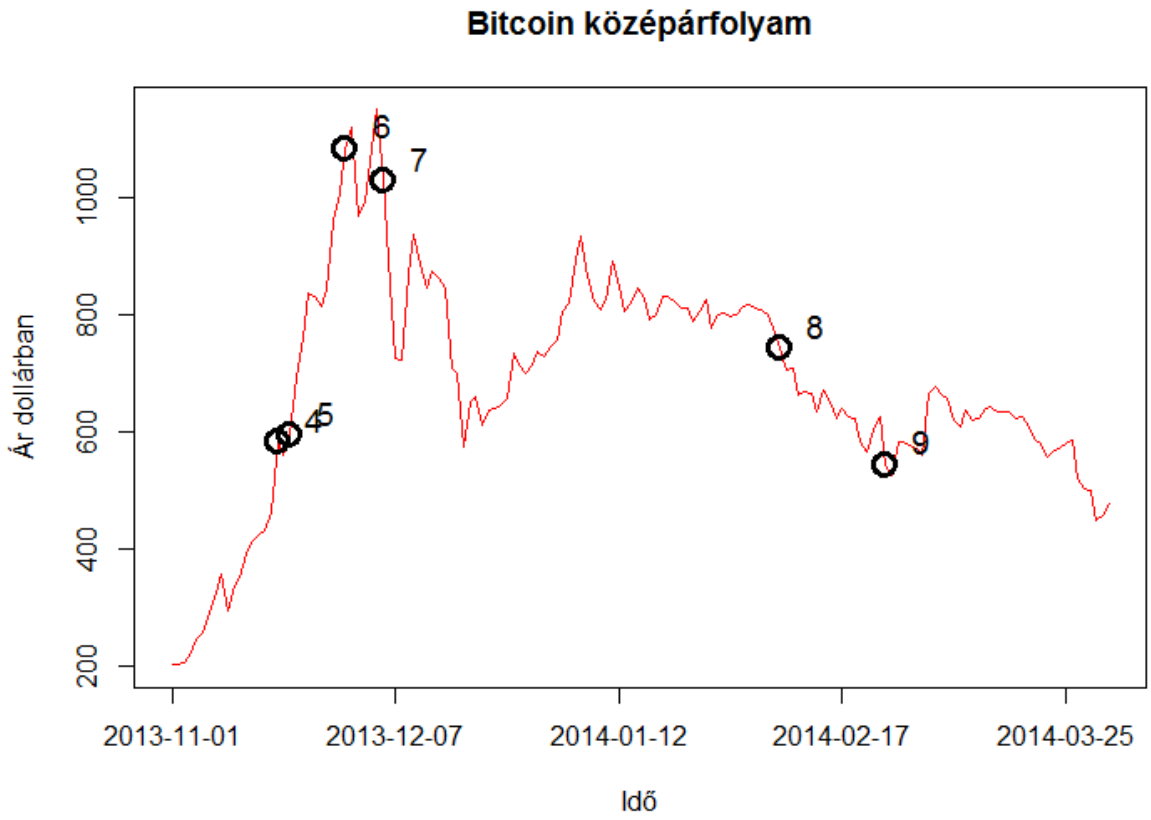
A bitcoin középárfolyama 2011. május és 2012.augusztus között, megjelölve a tárgyalt események időpontjai

1. Egy népszerű internetes portál felhívta a figyelmet egy anonim piactérre, amely főleg a fekete kereskedéssel foglalkozott. A picit több mint két évig működő Silk Road nevű piacon évi 15 millió dolláros forgalom lehetett körülbelül. Nagyságrendileg 10 000 különböző termékkel kereskedtek, amelyeknek a becslések szerint 70%-a valamilyen illegális drogféleség volt. Kihasználva a bitcoin anonimitását nehéz volt az oldalt felszámolni, de 2013 októberében az FBI lefoglalta a szervereiket.

2. Mint az árfolyamgörbén is látszik, van egy kisebb beszakadás, ennek oka, hogy sokáig az egész FX piacot domináló kereskedőportált, a Mtgoxot, 2011.június 19 - én feltörték. Ez a második típusú feltörések közé tartozott, a hackereknek sikerült megszerezniük a weboldal egy régebbi adatbázisát, amelyből adminisztrátori szintű hozzáféréshez jutottak az aktuális oldalhoz. Ezzel olyan nem létező bitcoin –dollár tranzakciókat tudtak becsempészni a Mtgox szervereibe, amellyel alaposan eltolták a bitcoin árfolyamát. Sőt a kiszivárgott adatbázisból olyan felhasználó jelszavakhoz is hozzájutottak, amelyek más piacokon első típusú csalásokat

eredményeztek, mert sok felhasználó azonos jelszavakat használt a különböző bitcoin kereskedő oldalakon.

3. Ez az esemény egy harmadik típusú csalás volt, amely abból állt, hogy egy személy 7% - os heti hozamot ígért bitcoinra, amit 8 hónapig sikerült tartania mégpedig úgy, hogy a hozamokat az új befektetők pénzéből finanszírozta. A végén természetesen összeomlott buborék, amit generált. Több százezer bitcoint sikkasztott így el. 2013-ban sikerült bíróság elé állítani csalás és piramisjáték szervezése vádjával.



11. ábra

A bitcoin középárfolyama 2013.november. és 2014 március. között, megjelölve a tárgyalt események időpontjai

4.Az Amerikai Egyesült Államok szenátusa meghallgatásokat tart a Silk Road ügyben és ez olyan média figyelmet kap, hogy az egész világon megindul az érdeklődés a bitcoin iránt.

5. Fellendülnek a legnagyobb kínai kereskedő honlapok. A jüan-bitcoin tranzakciók száma a duplájára emelkedik, a Mtgox dollár-bitcoin piac tranzakciókhoz képest.

6. A bitcoin eléri a mai napig felvett legmagasabb értékét, amely 1242 dollárt jelent bitcoinonként. Ezért egyértelműen a kínai élénkülés és a tömeges bitcoin vásárlás tehető felelőssé.

7. Ezt gyorsan meg is elégeli a Kínai Népköztársaság és nyilatkozatot tesz, hogy nem tekinti hivatalosan pénznek a bitcoint és betiltja a használatát az összes pénzügyi szervezetnél. Ez hatalmas törést okoz az árfolyamban: egy hónap alatt több mint felére esik vissza az ár.

8. A három vezető dollár FX piac nagy erejű DDos[3] támadásnak van kitéve, és ez leterheli szervereiket, a kereskedés akadozik, nehézkes.

9. Hirtelen elérhetetlen lesz a Mtgox piac szervere. Ezek után hamar kiderül, hogy a kereskedőház csődöt is jelent, 744 000 bitcoinnal nem tud elszámolni. Ez akkori árfolyamon több mint 400 millió dollárt jelent. Ez is nagy ingadozást okozott az árfolyamon, de közel sem akkorát, mint amit a kínai betiltások hoztak.

[3] Elosztott szolgáltatásmegtagadással járó támadás (Distributed Denial of Service, DDoS): informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. [22]

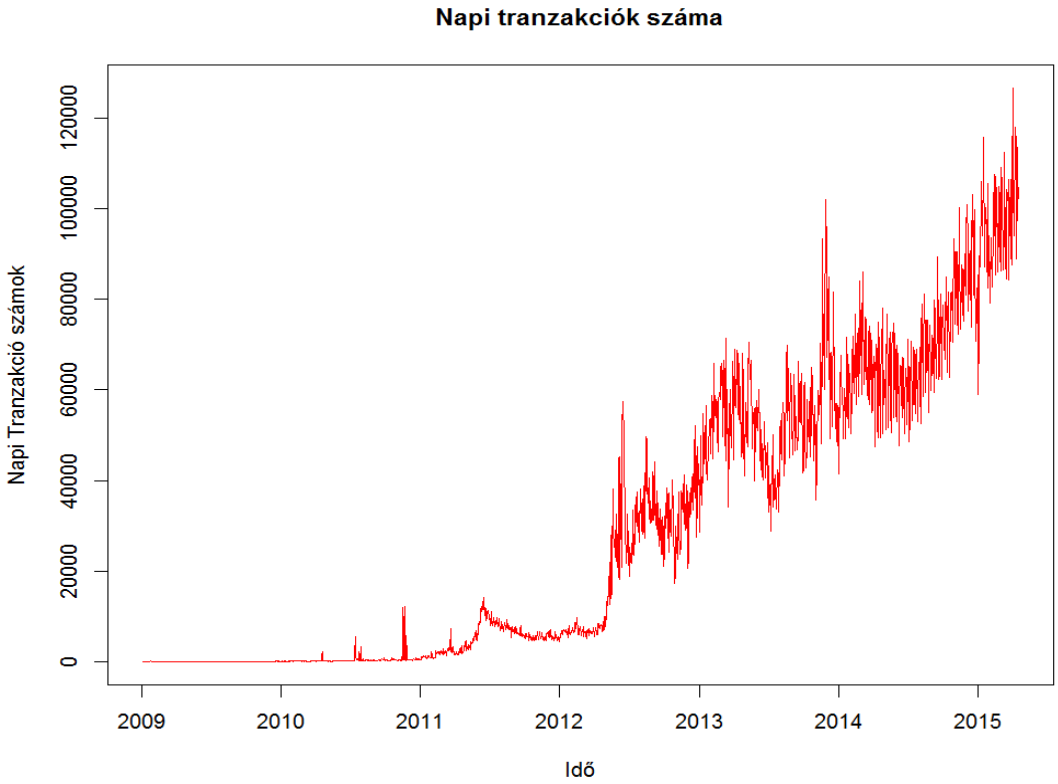
III. Fejezet

A bitcoinról elérhető információk [10]

Miután áttekintettem a bitcoin elméletbeli működési elvét, valamint a vele kapcsolatos közgazdasági problémákat és botrányokat, a következőkben szeretném bemutatni milyen információk érhetőek el a bitcoinról, milyen módszerekkel érdemes vizsgálni azokat.

A dolgozat elkészültének pillanatában a bitcoin hálózat 352 000 blokkot tartalmaz. A bitcoin népszerűségének talán legszemléletesebb példája a piacon lévő összes bitcoin értéke USA dollárban az idő függvényében, valamint a napi tranzakciók száma.

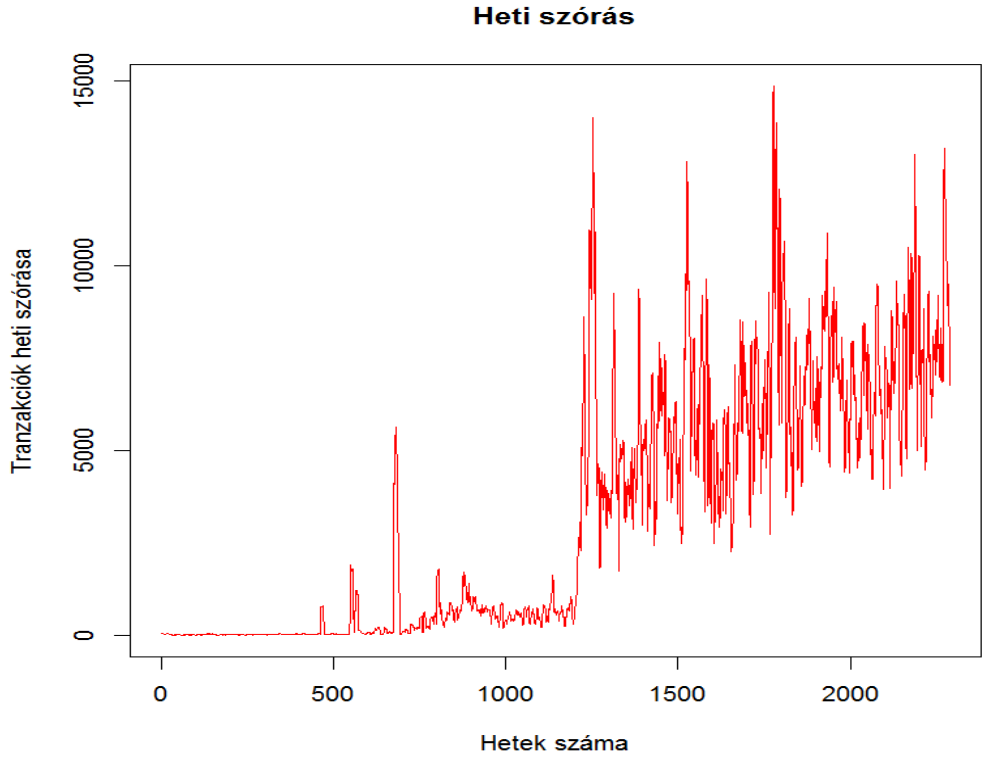
12. ábra
A forgalomban lévő összes bitcoin dollárban kifejezett értéke az idő függvényében



13. ábra
A bitcoin-bitcoin tranzakciók napi száma az idő függvényében

Az elmúlt egy évben átlagosan naponta 78 933 bitcoin-bitcoin tranzakciót bonyolítottak le. De mint a fenti ábrából is láthatjuk még mindig erősen növekvő ez a trend (az elmúlt 100 napban már 98 213 az átlag).

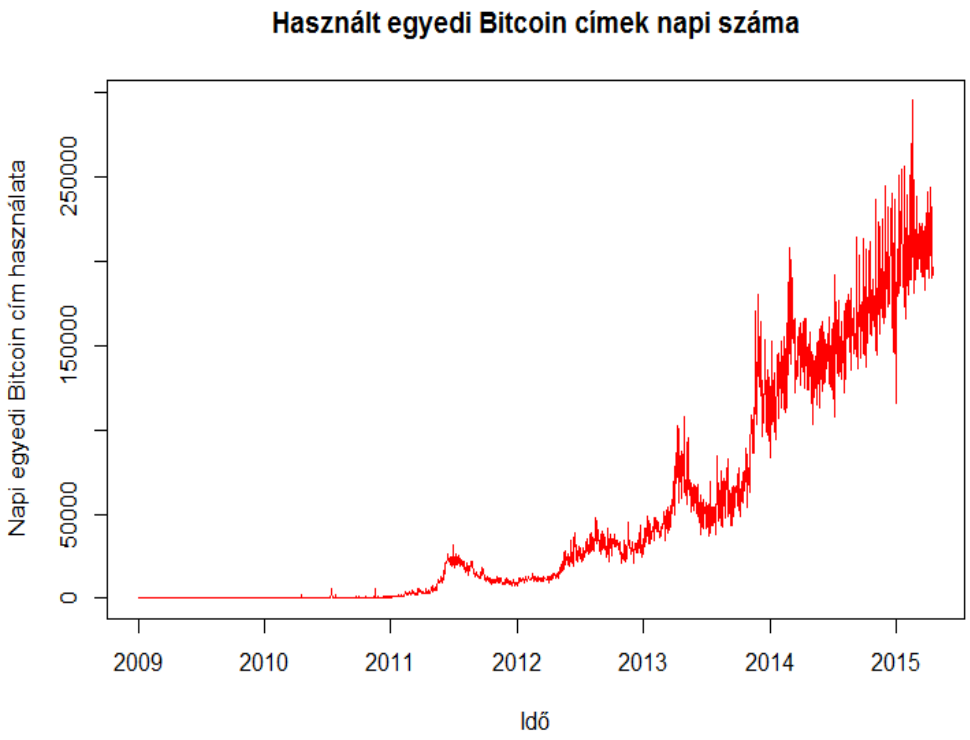
De következő ábra tanulsága szerint a tranzakciók szórása időben közel azonos ingadozást követ: az egyetlen hatalmas váltás a bitcoin kínai berobbanása következtében látható.



14. ábra

A bitcoin-bitcoin tranzakciók heti szórása az idő függvényében

Hasonló drasztikus emelkedést láthatunk azon egyedi bitcoin számlák címeinek a számában, amelyek az adott napon tranzakcióban részt vettek.



15. ábra
A forgalomban lévő egyedi bitcoin címek száma az idő függvényében

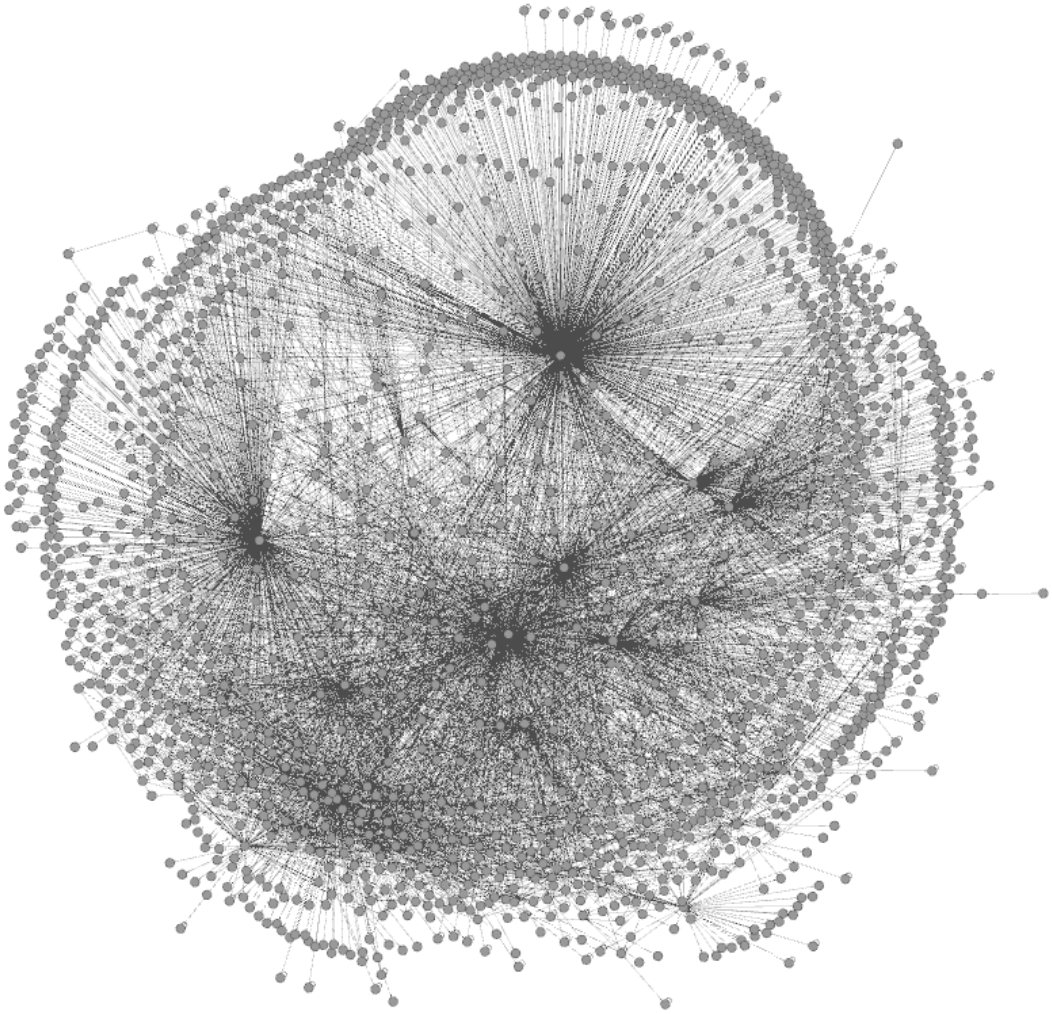
Fontos itt megemlíteni, hogy bármilyen számlatulajdonos akárhány egyedi címet generálhat. Ez nagyon megnehezíti az adatok elemzését, mert az ember olyan problémába ütközik, hogy nem tudhatja biztosan, hogy a bitcoin cím milyen valós személyhez, vagy csoporthoz köthető.

Korábban már láthattuk, hogyan épül föl egy blokk, de az elemzés átláthatóságának érdekében összefoglalom, hogy milyen adatok menthetőek ki a peer to peer hálózatból. Nyilvános a teljes Blockchain ami tartalmazza:

- az adott blokk megfejtett hasító értékét
- az előző blokk hasító értékét
- ha nem az utolsó blokkot nézzük, akkor a következő blokk hasító értékét
- a blokk készítésének időpontját
- a blokkhoz tartozó proof to work nehézségét
- a blokkban található tranzakciók számát
- a blokk tranzakcióinak összvolumenét
- a blokk adatméretét
- minden tranzakció bemenő és kimenő címét és azonosítóját
- az egyes címek bementeti és kimeneti bitcoin értékét

Ez számunkra egy hatalmas, időben dinamikusan fejlődő, súlyozott, irányított gráf adatbázist biztosít. Szinte kezelhetetlen méretű adatbázisról beszélhetünk. 65 955 849 tranzakció szerepel ebben a gráfban 115 877 664 egyedi számlacím között. A tranzakciók számának növekedésével az adatbázis mérete is nagy gyarapodáson esett át. Az elméleti tárgyalásnál jósolt alacsony méretigénynek sokszorosával nézünk szembe, bár valóban nem olyan mértékben növekszik az adatbázis, hogy tárhely problémákat okozzon, viszont ennek a komplex rendszernek a vizsgálatát igencsak megnehezíti.

A tranzakciós gráf egy algráfjának vizualizációja



***16**. ábra*
A tranzakciós hálózat hosszútávon aktív felhasználóira szűrt gráfjának megjelenítése

A fenti ábrán a hálózat körülbelül 1700 hosszútávon aktív felhasználóra szűrt hálója látható. Egy pont mögött sok olyan cím található összeejtve, amelyek valószínűleg egyazon felhasználóhoz tartoznak.

IV.Fejezet

Matematikai fogalmak [11] [12] [13] [14]

Az adatok szűrésének és feldolgozásának ismertetése előtt szeretném összegyűjteni azokat a gráfelméleti fogalmakat, amelyeknek fontos szerepe lesz az elemzésekben.

Definíció:

$G = (V, E, \varphi)$ *gráf, ahol* V *a csúcsok halmaza,* E *az élek halmaza,*

φ *illeszkedés reláció:* $\varphi \subseteq E \times V, v \in V \; e \in E$

v *illeszkedik ez* e *élre, ha* $v \in \varphi(e)$

Definíció:

$G = (V, E, \Psi)$ *gráf, ha* V, E *halmazok,* $\Psi: E \to V \times V$

$\Psi(e) = (v, v')$, *ahol* v *ez* e *kezdőpontja és* v' *a végpontja*

Definíció:

Egy gráf fokszámeloszlása: $p(k) = \sum_{v \in V \mid \deg(v)=k} 1$

Egy gráf kumulatív fokszámeloszlása: $\Pi(k) = \sum_{k'=k}^{\infty} p(k')$

A fokszámeloszlás megmutatja, hogy milyen gyakorisággal fordulnak elő a gráfban különböző fokszámú csúcsok.

Definíció:

Egy gráf fokszámeloszlása hatványeloszlást követ, ha

$\Pi(k) \sim k^{-\alpha}$

Definíció:

G Gini koefficiens, ha $G = \frac{2\sum_{i=1}^{n} i x_i}{n\sum_{i=1}^{n} x_i} - \frac{n+1}{n}$

$ahol\ x_i\ egy\ n\ hosszúságú\ monoton\ növekvő\ minta\ x_i < x_{i+1}$

$egy\ hatványeloszlású\ gráf\ esetén\ a\ G = \frac{1}{2\alpha - 3}$

Definíció:

$C\ átlagklaszterezettségi\ koefficiens\ ,ha\ C = \frac{1}{N}\sum_v \frac{\Delta_v}{\frac{d_v(d_v-1)}{2}}$

Ez a szám a megvalósuló háromszögek arányát mutatja a gráfban az összes lehetséges háromszöghöz képest.

Definíció:

$r\ Pearson - féle\ korrelációs\ koefficiense\ \ a\ gráfnak, ha$

$$r = \frac{\sum_e (j_e^{out} - \overline{j_e^{out}})(k_e^{in} - \overline{k_e^{in}})}{L\sigma_{in}\sigma_{out}}$$

$ahol\ j_e^{out}\ a\ kimeneti\ fokszáma\ a\ csúcsnak\ az\ él\ kezdeti\ pontján,$

$k_e^{in}\ a\ bementi\ az\ él\ végpontján$

A Pearson féle korrelációs koefficiens lineáris kapcsolatot mér a változók között.

Definíció:

$Spearman - féle\ korrelációs\ koefficiens\ a\ rangsorolt\ változók$

$Pearson\ korrelációja\ \ p = 1 - \frac{6\sum_{i=1}^{n}(j_e^{out} - k_e^{in})_i^2}{n(n^2-1)}$

A komplex hálózatok fejlődését sokféleképpen lehet modellezni. Az elemzésünkben Barabási Albert László és Albert Réka által kidolgozott, úgynevezett preferential attachment modellt alkalmaztunk, amelyek sok esetben modellezik jól a valós hálózatok növekedését. A modell szerint úgy növekszik a hálózat, hogy kezdetben adott egy legalább két csomópontú hálózat, amelyben minden csúcshoz legalább egy él vezet. Minden egyes lépésben egy újabb csúcsot adunk hozzá, melyet egy-egy éllel kapcsolunk valahány véletlenszerűen választott régi csúcshoz úgy, hogy a kiválasztás valószínűsége arányos a régi csúcsok pillanatnyi fokszámával.

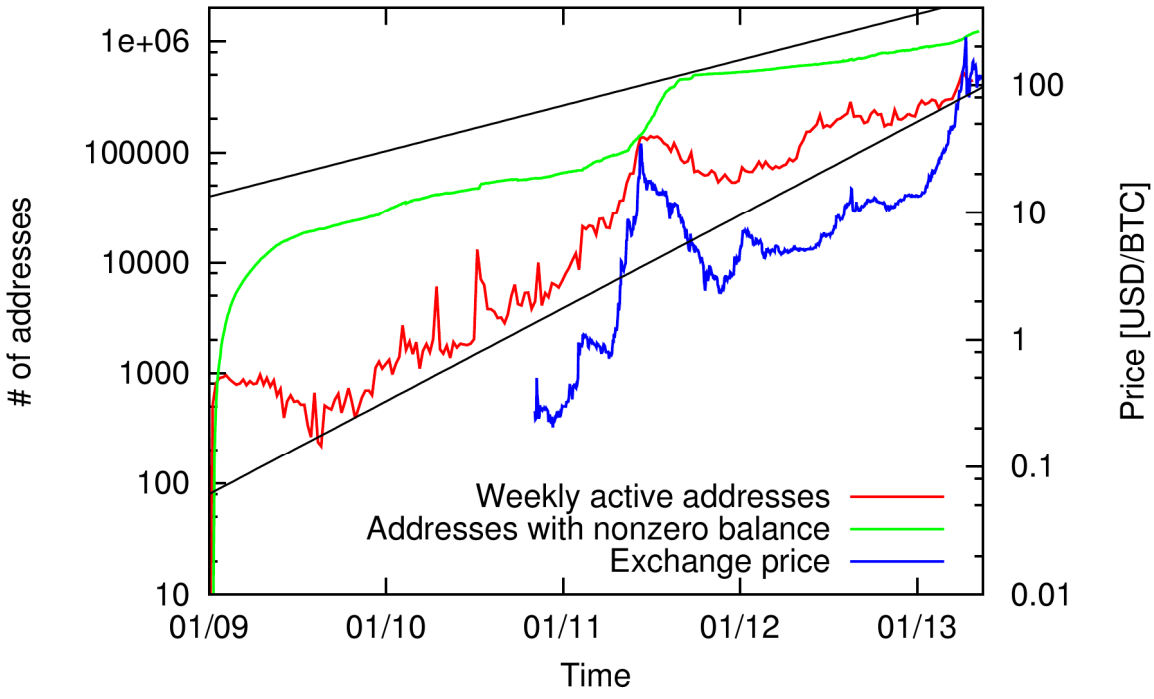
$$p_i = \frac{k_i}{\sum_j k_j}$$

V. Fejezet

A tranzakciós hálózat elemzése [15]

Az adatok SQL adatbázisba rendezése után a hálózat növekedését oly módon lehet vizsgálni, hogy a hálózat karakterisztikájának változását vizsgáljuk az idő függvényében. Itt időben két szakaszra lehet bontani a bitcoin korai időszakát. Az első szakasz még kísérleti jellegű korszaknak tekinthető, ami a kezdetektől 2010 végéig tartott. Ekkor még számottevő kereskedés nem történt. A változás és hálózat extrém növekedése már az alábbi ábrán is jól látható.

A bitcoin számlák mennyisége a korai szakaszban



17. ábra

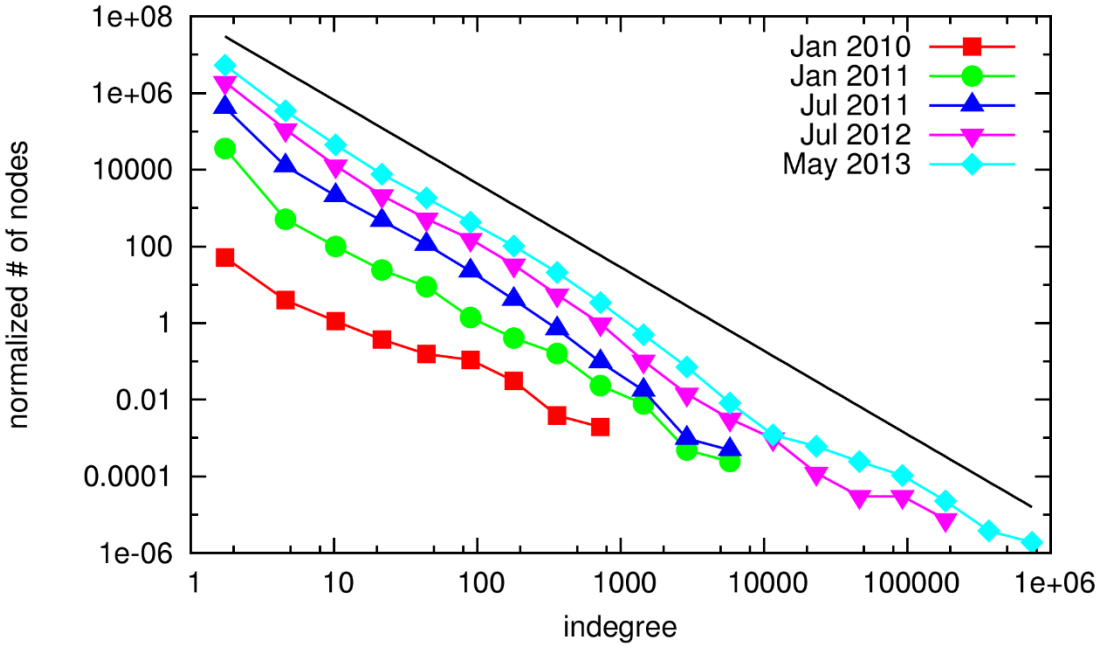
Az idő függvényében látható: a hetente aktív címek száma,a nem nullaegyenlegű számlák száma és az árfolyam

Logaritmikus skálán ábrázolva zölddel láthatjuk azoknak az egyenlegeknek a számát, amelyek nem üres címeket tartalmaznak. Pirossal azoknak a címeknek a számát, amik heti legalább egy tranzakcióban részt vettek. Kékkel pedig a bitcoin akkori legjelentősebb tőzsdén jegyzett középárfolyamát. Láthatjuk, hogy a növekedés sokszor meghaladja a 188 napos karakterisztikus idejű exponenciális trendet (meredekebb fekete).

Mivel a hálózat nem egyéni pénztárcánként kezeli az egyenlegeket, ezért a változásra a bemeneti összegek és a kimeneti összegek különbségeként kell tekintenünk (a korábban tárgyalt visszautalásos elvvel összhangban).

A hálózat növekedését a fokszámeloszlás vizsgálatával folytatjuk. Az egyes bemeneti és kimeneti fokszámeloszlásokat -mint sok más valós hálózat esetében- modellezhetjük hatványfüggvénnyel a nagymértékű heterogenitás okán.

A tranzakciók bemeneteinek fokszámeloszlása

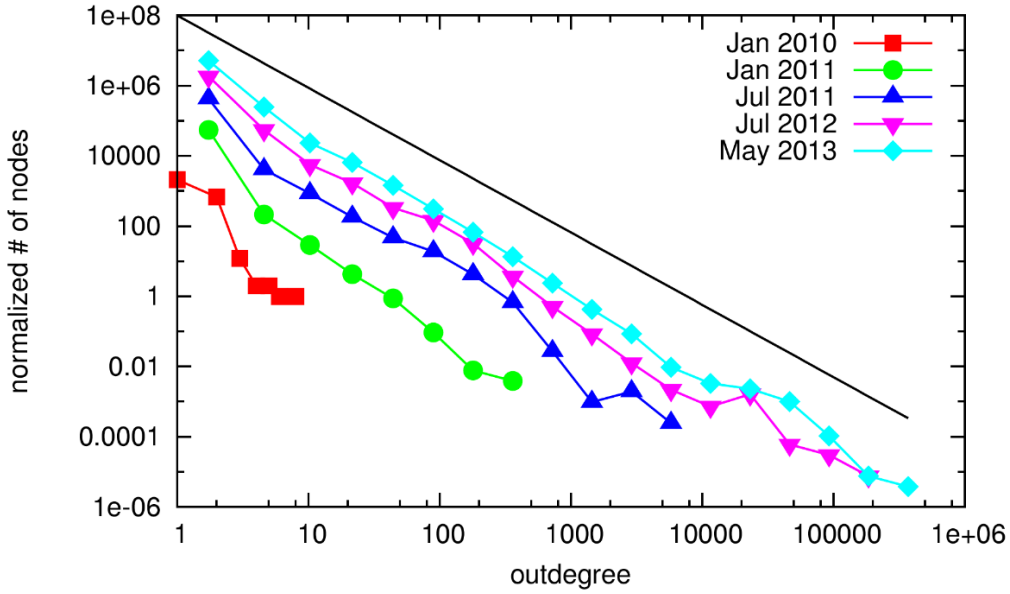


18. ábra
A tranzakciós gráf bemeneti fokszámeloszlása logaritmikus skálán

A fenti ábrán logaritmikus skálán láthatjuk a bemeneti fokszámeloszlását az adatoknak, míg az alsón a kimenetit. A különböző színek a különböző időszakokat mutatják. A kezdeti szakaszban nagy hibával mondható hatványfüggvénynek az eloszlás, de a piacon való megjelenéstől kezdve szignifikánsan nem változik a kitevő. A fekete vonalak jelentik a teljes adatsorra illesztett görbét.

$$p_{be}(k_{be}) \sim k_{be}^{-2.18} \qquad p_{ki}(k_{ki}) \sim k_{ki}^{-2.06}$$

A tranzakciók bemeneteinek fokszámeloszlása

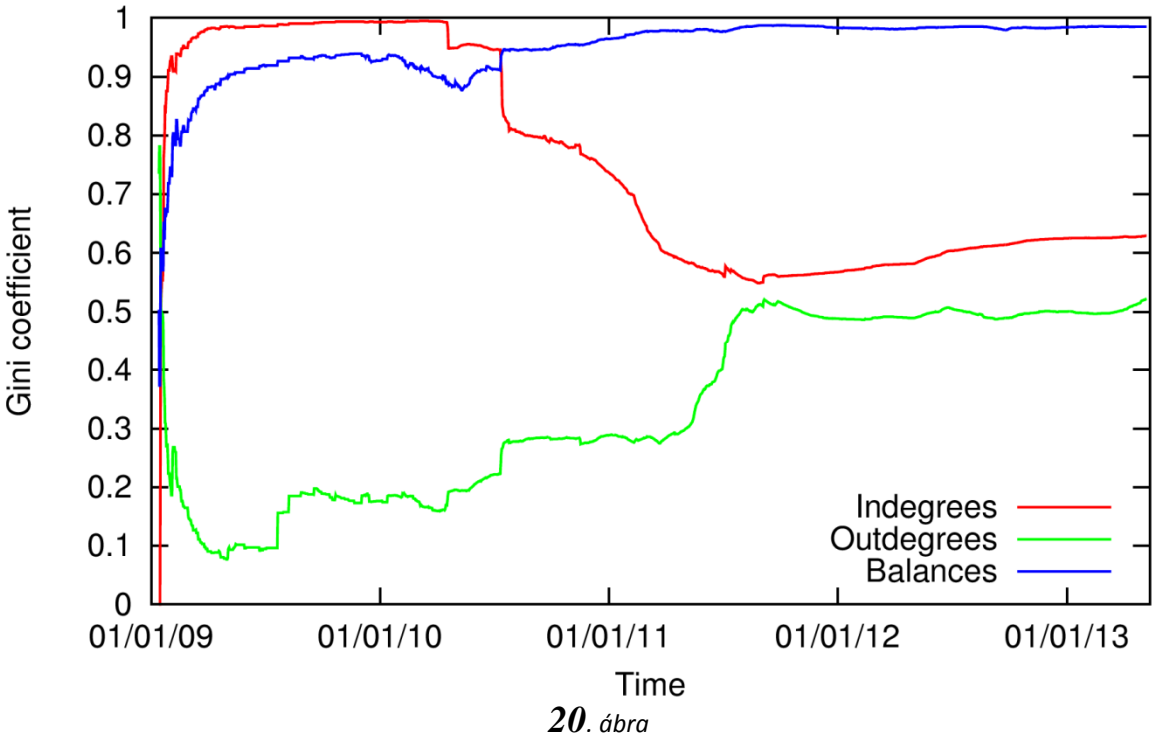


19. ábra

A tranzakciós gráf kimeneti fokszámeloszlása logaritmikus skálán

A már definiált Gini együtthatóval szokás jellemezni azon vagyon eloszlásokat, amelyekben nagy egyenlőtlenségek találhatóak. Számunkra is alkalmas az empirikus eloszlásunk heterogenitásának vizsgálatára. A 0 Gini együttható jelenti a tökéletesen egyenlő vagyon elosztást és az 1, hogy egy pontban összpontosul a vagyon.

Gini együtthatók időbeli változása



***20**. ábra*

A bemenetek, kimenetek és egyenlegek Gini együtthatói az idő függvényében.

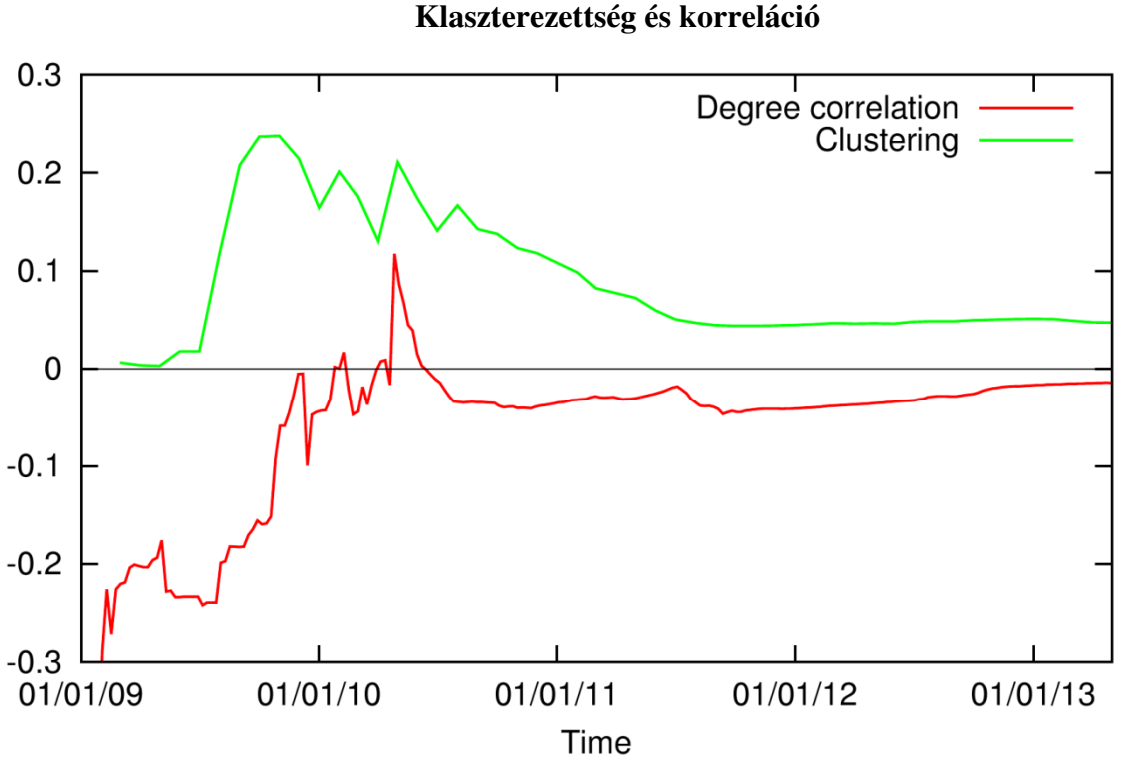
A fenti ábrán jól látszik a hatalmas váltás a piacra vonulás időpontja körül. A kísérleti szakaszban a hatalmas különbséget a bemeneti és kimeneti Gini együtthatóban az okozza, hogy a hálózat szereplői tulajdonképpen csak a blokkosításért járó teremtett pénz utalásaival dominálják a tranzakciókat - mivel kereskedni nem igazán lehetett - ezért senkinek nem állt érdekében, hogy ne egy-két számlán tárolják szinte az összes akkor létező bitcoint. A kereskedés beindulása után az együtthatók bekonvergáltak körülbelül kontstans értékre.

$$Gini_{be} = 0.629\ Gini_{ki} = 0.521$$

Ez szintén a nagymértékű heterogenitást támasztja alá.

A Pearson korrelációs együtthatóval a gráf szerkezeti tulajdonságáról kapunk információt. Ha az együttható pozitív, akkor a gráf asszortatívnak tekinthető, amely azt jelenti, hogy a nagy élszámú csúcsok gyakran kötődnek szintén nagy élszámú csúcsokhoz. Ha negatív, akkor disszortatívnak nevezzük, amely a valós hálózatok gyakori tulajdonságát tükrözi: miszerint, a nagy élszámmal rendelkező csúcsok a kis élszámúakhoz kötődnek gyakrabban.

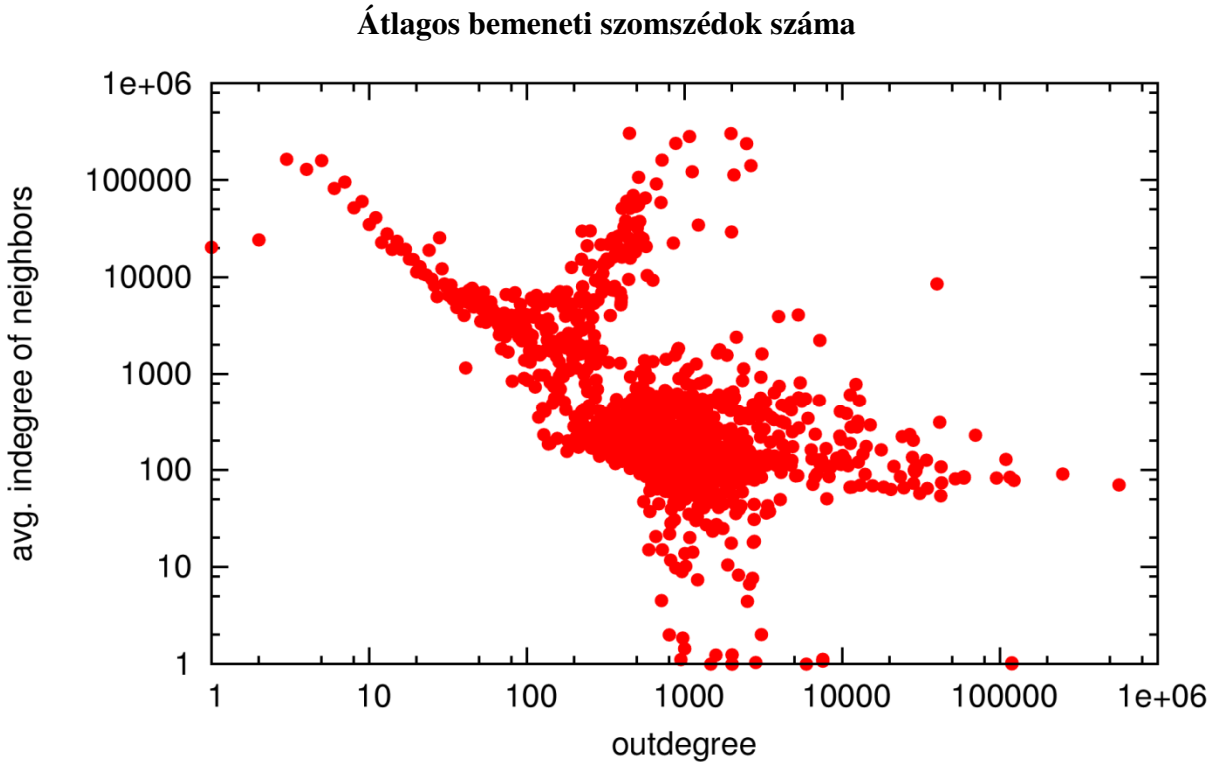
A hálózat klaszterezettségét pedig az átlagklaszterezzetségi együtthatóval jellemezhetjük, amely - ahogy már fentebb tárgyaltam - a háromszögek sűrűségét méri a gráfon belül.



21. ábra

A klaszterezettség és a korreláció az idő függvényében

A fenti ábrán ismét látható a nagy különbség a kezdeti szakasz és a piacra lépés utáni szakasz között. A kezdeti időszakban a nagy klaszterezettségi együttható ingadozása a nagyszámú saját címek közötti tranzakciókkal magyarázható. A negatív korreláció a skálafüggetlen gráfokra jellemző tulajdonságot mutat [16], de ennek alátámasztása érdekében megvizsgáljuk az átlagos bemeneti szomszédok számát a kimeneti élszámok függvényében.



22. ábra
Átlagos bemeneti szomszédok száma a kimeneti élszámok függvényében

A fenti ábra alapján szintén kijelenthetjük, hogy erős a disszortativitás és egy véletlen gráfnál jóval magasabb klaszterezettség jellemzi a tranzakciós gráfunkat.

Ahhoz, hogy jobban megértsük miért illeszkedik ennyire jól egy hatványfüggvény a fokszámeloszlásra, a halózat időbeli fejlődését kell modelleznünk. Az előzőekben tárgyalt preferential attachment modell alkalmas arra, hogy a hálózat mikrodinamikáját modellezzük vele.

Ha modellnek egy nem lineáris preferential attachment modellt választunk, a következő módon tudjuk tesztelni az adatbázisunkon. Annak a valószínűsége, hogy egy új tranzakciós él indul ki a v-edik csúcsból:

$$p(k_v) = \frac{{k_v}^{\alpha}}{\sum_w {k_w}^{\alpha}}$$

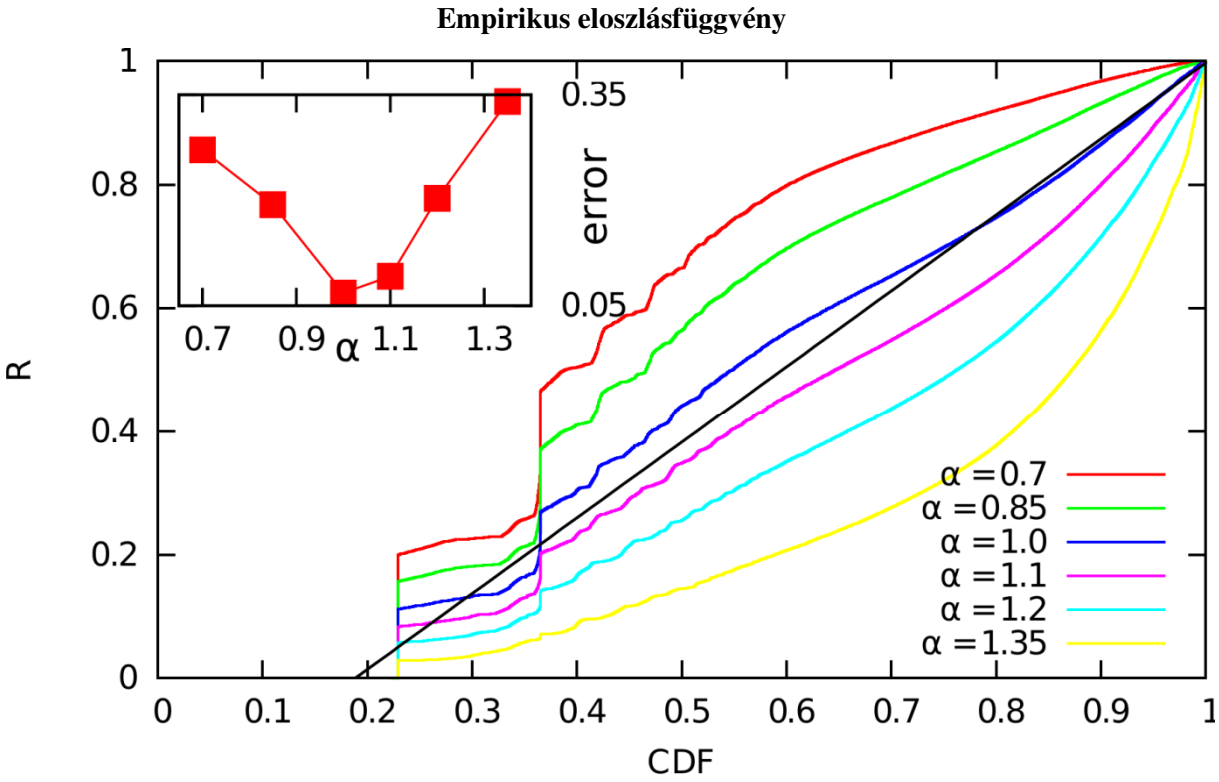
Ahol a k_v a v-edik csúcshoz tartozó bemenő élek addigi száma. Annak a valószínűsége, hogy egy új él kerül bármely k élszámú csúcshoz:

$$\Pi(k) \sim n_k(t)p(k)$$

Ahol $n_k(t)$ az adott pillanatban k éllel rendelkező csúcsok száma a gráfban. Ahhoz, hogy ezt vizsgáljuk a hálózaton, a $\Pi(k)$ időfüggőségének problémájába ütközünk. Ahhoz, hogy ezt a problémát feloldjuk, a $\Pi(k)$-t egy egyenletes eloszlásba transzformáljuk a következő rangfüggvény segítésével:

$$R(k,t) = \frac{\sum_{j=0}^{k} n_j(t) j^{\alpha}}{\sum_{j=0}^{k_{max}} n_j(t) j^{\alpha}} = \frac{\sum_{k_v<k} {k_v}^{\alpha}}{\sum_v {k_v}^{\alpha}}$$

Ez t független és egyenletes eloszlású a [0,1] intervallumon. Ha megfelelő alfával vesszük fel az eloszlásfüggvényt, akkor egy egyenest kell kapnunk. Az exponens értéke úgy határozható meg, hogy az empirikus eloszlást összehasonlítjuk az egyenletessel a Kolmogorov-Smirnoff távolság kiszámításával. Mint az alábbi ábrán jól látható, az α 1 körüli megválasztásával nem tökéletes, de jó egyezést kapunk. Tehát állíthatjuk, hogy a preferential attachment modellel megmagyarázható a fokszámeloszlás szerkezet. Ez önmagában még nem magyarázza meg a klaszterezettségét a hálózatnak, de így is állíthatjuk, hogy a bitcoin is mutatja azt a skálafüggetlen tulajdonságot, amelyet annyi valós hálózat felépítésénél már tapasztaltunk.(Szociális hálók, internet, tudományos publikációk hálózata stb.) [17]



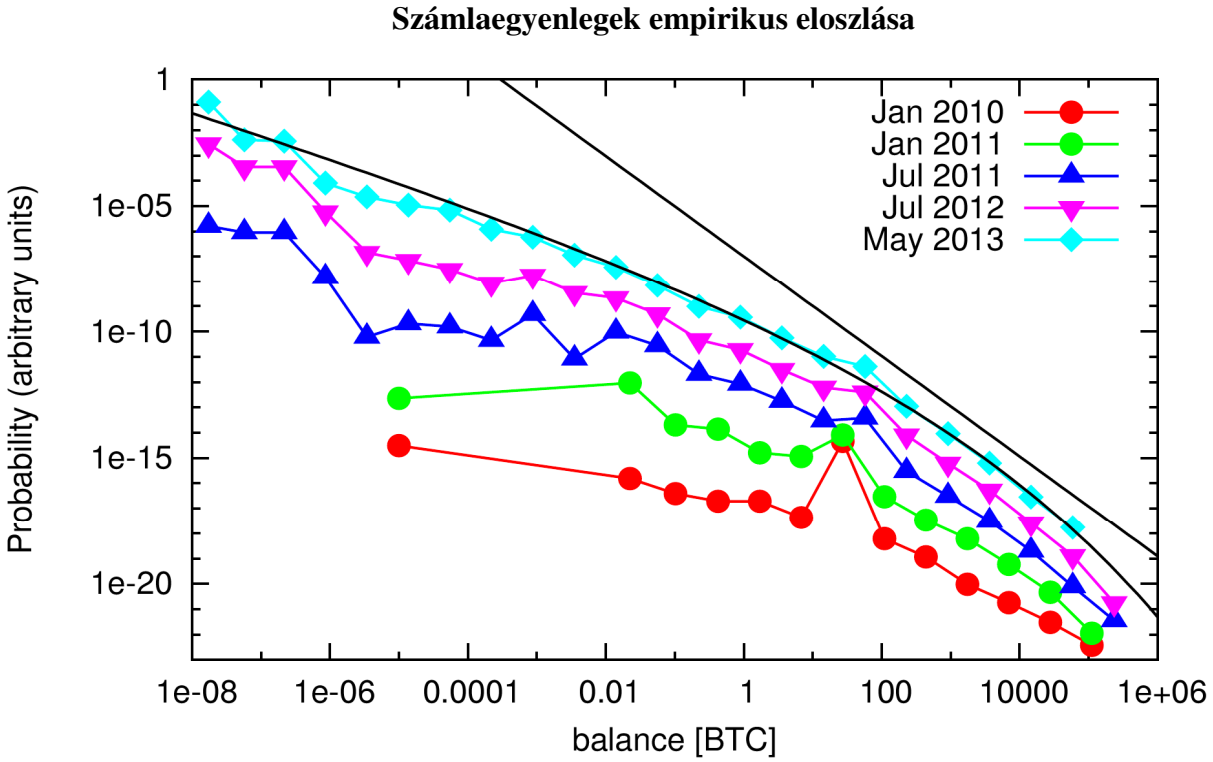
23. ábra

Az α különböző értékei mellett az empírikus eloszlásfüggvény és a hiba az α függvényében

A hálózat lehetőséget ad, hogy vizsgáljuk a közgazdaságtanban gyakran emlegetett Pareto vagyonosodási elvet [18]. Az elv úgy hangzik, hogy egy olyan Pareto eloszlást követ a vagyon az egyes szereplők között a világban, hogy a leggazdagabb 20%-nál található a vagyon 80%-a. A hálózatban szereplő címek egyenlegét vissza lehet fejteni egy adott pillanatban az odamutató befele és kifele mutató tranzakciók különbségeként. Az alábbi ábrán látható az empirikus eloszlása a számlaegyenlegeknek különböző időszakokra visszanézve. A Pareto arányt a bitcoin hálózatban úgy lehetne megfogalmazni, hogy a bitcoin számlák 6.28% - a birtokolja a bitcoinok 93.72%-át. Az eloszlás azonban Pareto eloszlással nem jól modellezhető. Sokkal jobban illeszkedik egy nyújtott exponenciális eloszlásra.

$$P(b) \sim b^{-\gamma} e^{-(ab)^{1-\gamma}}$$

Ahol a γ=0.873 az a pedig a=8014BTC^{-1} adódik. A 20. ábrán láthatjuk, hogy a Gini együttható a hálózat teljes vizsgált időtartamán nagyon magas.



24. ábra

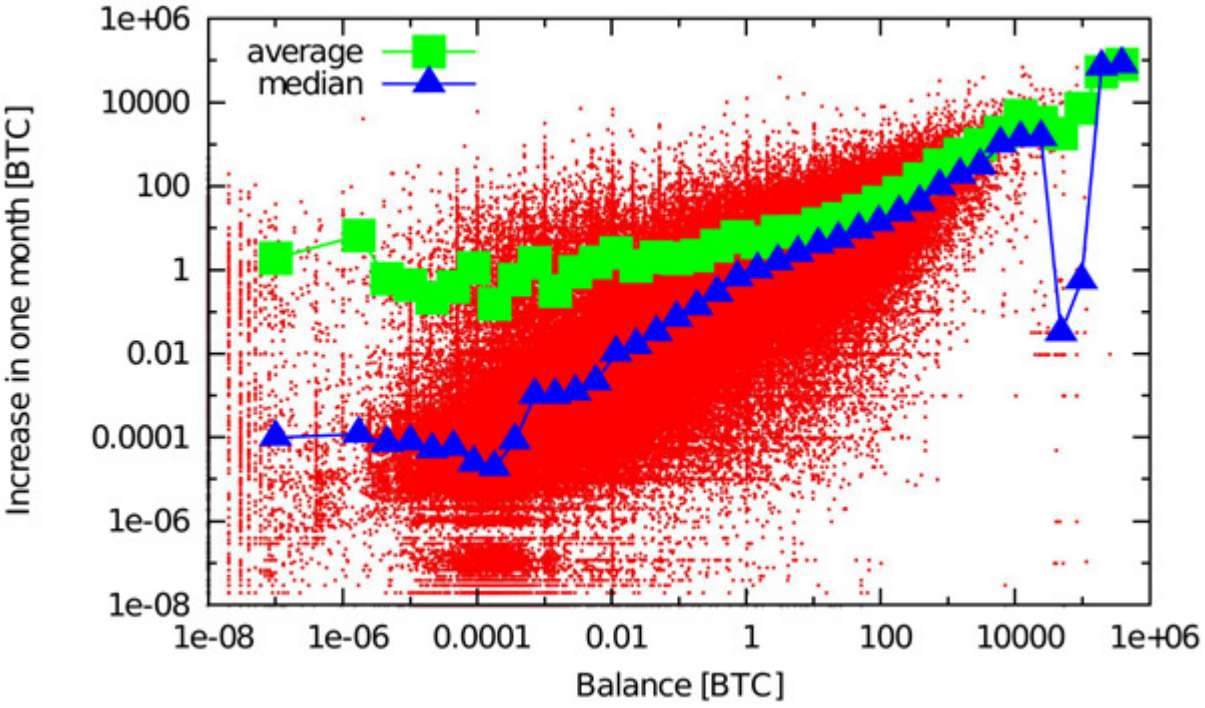
A számlaegyenlegek empírikus eloszlása különböző időszakokra nézve

Az ilyen nagymértékű heterogenitást az egyenlegek tekintetében is lehet magyarázni a preferential attachment hálózatfejlődési modellel, amelynek közgazdaságtani analógiája Robert C. Merton szociológus Máté effektusnak nevezett megfigyelése, amelyet csak „rich get richer" néven szoktak emlegetni. [19] Nevét pedig Máté evangéliumának 25:29 verséről kapta:

„Mert mindenkinek, a kinek van, adatik, és megszaporíttatik; a kinek pedig nincsen, attól az is elvétetik, a mije van."

Ezt az elvet vizsgálhatjuk oly módon, hogy egyhónapos időablakokban tekintjük a számlaegyenlegek változását az egyenlegek függvényében. Az alábbi ábrán erős pozitív korrelációt figyelhetünk meg a számlaegyenlegek vagyonossága és a vagyon növekedése között. Az ábra logaritmikus, tehát ismét egy hatványfüggvény az, amely jól közelíti a növekedés trendjét. A kitevő közelítőleg 0.857.

Vagyonnövekedés

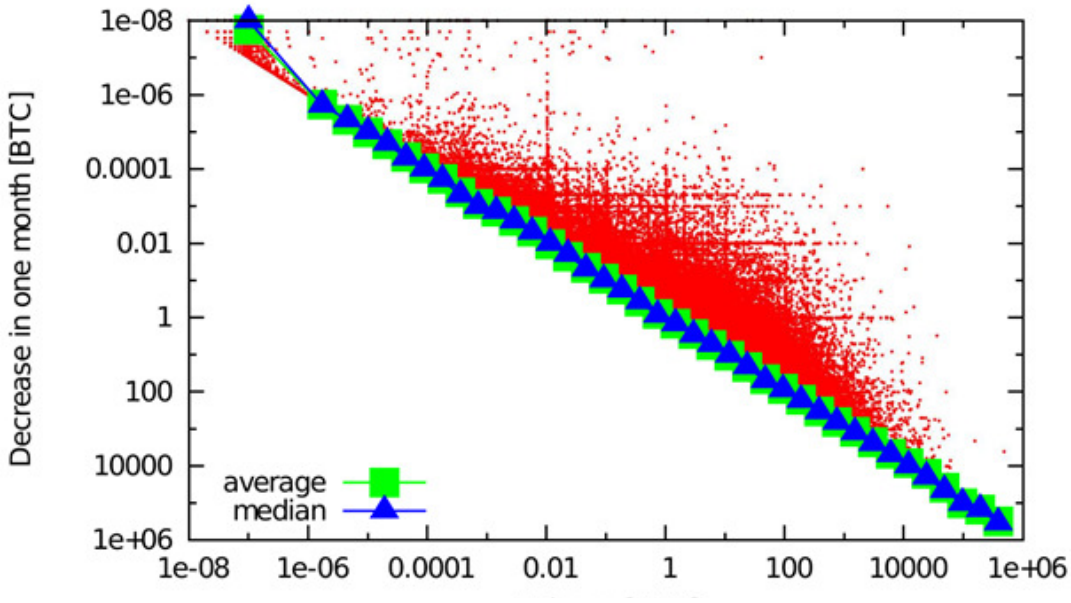


25. ábra

A számlák havi vagyon növekedése a kezdeti egyenleg függvényében

A számla csökkenéseknél arra lehetünk figyelmesek, hogy meglehetősen sok számla ürül ki teljesen. Ennek az oka az anonimitási lehetőség a bitcoin hálózatban. Sok számlatulajdonos forgatja meg a pénzét a saját számlái között, hogy még nehezebben lehessen beazonosítani a tulajdonos kilétét.

Egyenleg csökkenés



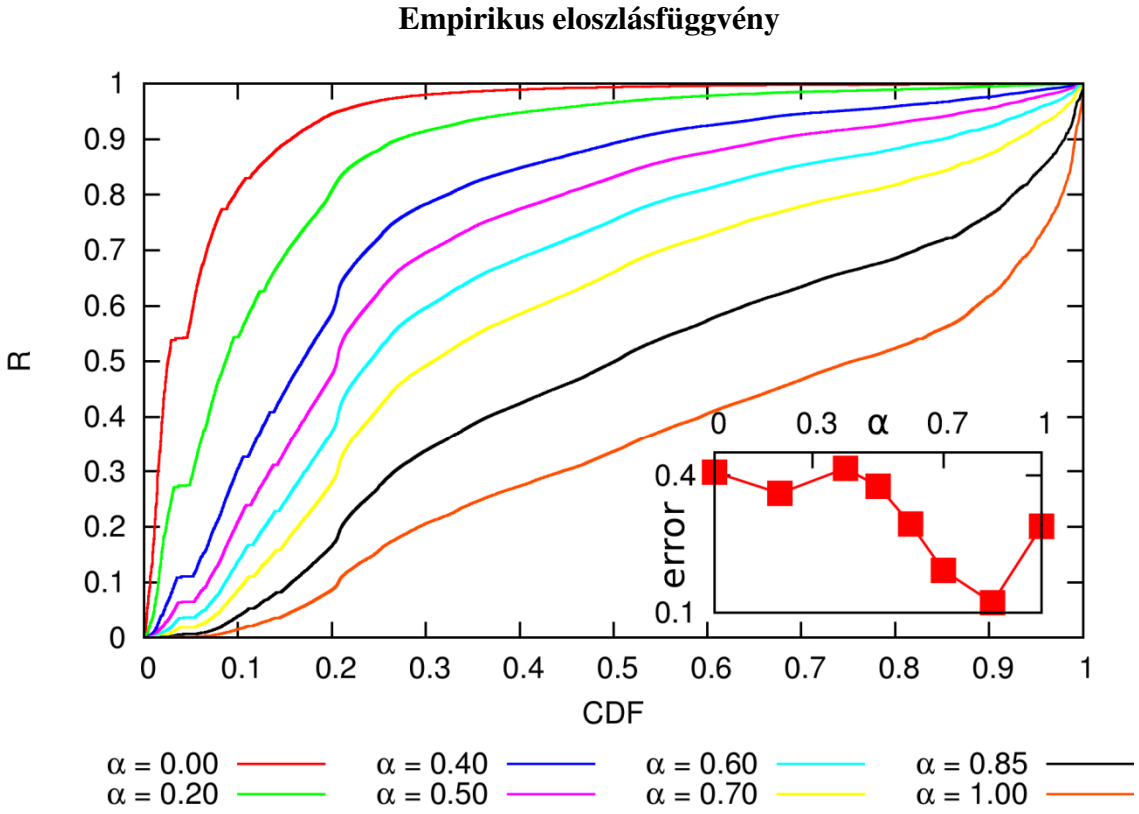
26. ábra

Az egyenlegek havi csökkenése a kezdeti értékek függvényében

Felmerülhet bennünk a kérdés, hogy lehetne-e nyomon követni a személyeket nem számlaazonosító útján, hanem a számlatulajdonos számítógép használati helye - az ip címe- alapján. Erre sajnos az egész hálózatra kiterjedően nincs lehetőség, mert aki az anonimitást szorgalmazza, az gyakran kombinálja az új számla generálást úgynevezett TOR típusú internet használattal. Ez egy speciális proxy hálózat, amelyet hagyma hálózatnak is szokás nevezni, mert sok különböző titkosított proxy csatornán keresztül teremt kapcsolatot a számítógép és az internet között. Ezen proxy rétegeken pedig a pontos szerver utakat rövid időn belül variálják, ezért az ip alapu helymeghatározás lehetetlenné válik, mert külső szemmel a felhasználó folyamatosan változtatja az ip címét az egész világon össze-vissza.

Ugyanúgy alkalmazható a vagyonosodás modellezéséhez az előző preferential attachment hálózatfejlődési modell, viszont kicsit módosított elven. Míg korábban egy tranzakció pontosan eggyel növelte egy csúcs éleinek számát, itt úgy kell tekintenünk a fejlődésre, mint a csúcsokba futó különálló és egyidejű tranzakciós élekre, amelyek pont az adott mennyiséggel növelték az adott számla értékét.

Ismét kiszámítható különböző α paraméter mellett az empirikus eloszlásfüggvény. Az előző verzióhoz képest viszont az alábbi ábrán látható, hogy kevésbé mondható el az, hogy egy paraméterrel leírható lenne a valószínűség. A legjobb egyezést $\alpha = 0.85$ környékére lehet tenni. Korábbi kutatások arra a következtetésre jutottak, hogy ilyen szublineáris eredményeket produkálnak a stacionárius nyújtott exponenciális fokszámeloszlású gráfok az ilyen hálózatfejlődési modellekben.

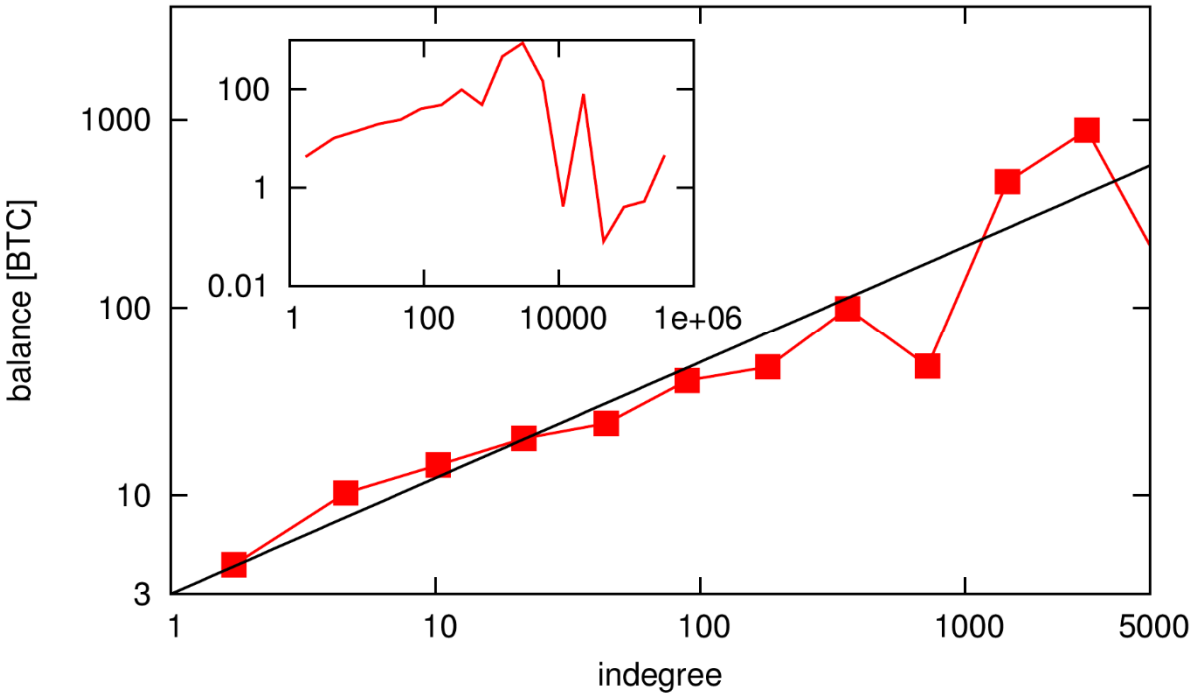


27. ábra

Az α különböző értékei mellett az empírikus eloszlásfüggvény és a hiba az α függvényében

Természetesen a két eredmény nem választható el egymástól, hiszen a gráfok ugyanazon adatbázisból lettek felépítve. A következő ábrán logaritmikus skálán szerepel a fokszám függvényében az egyes csúcsok egyenlege. Alacsony fokszámoknál jól közelíthető egyenessel a kapcsolat. Itt is egy hatványfüggvény a kapcsolat, mégpedig α=0.61 paraméterrel. A teljes tartományra ez azért nem igaz, mert a hálózat magas fokszámú pontjai nagyon fluktuálnak. Ennek oka, hogy összesen csak 75 csúcsnak van extrém magas fokszáma, ezért az átlagos egyenleget nagyon eltorzítják.

Bemeneti fokszám és egyenleg kapcsolata



28. ábra

Az egyenlegek a fokszám függvényében: 1-5000 fokszámig és a teljes gráfon

VI. Fejezet

A tranzakciós hálózat főkomponens-analízise [20]

Eddig a vizsgálatok csak és kizárólag a bitcoin-bitcoin számlák közötti tranzakciókra vonatkoztak. Közgazdasági szempontból fontos kérdés az is, hogy mennyire tekinthető hatékonynak a bitcoin devizapiaca. A hatékony piacok elmélete úgy szól, hogy a piacon megfigyelhető ár tükrözi az elérhető információkat. A pénzpiacokhoz képest sokkal több információ nyilvános teljes egészében, ezért felmerül a kérdés, hogy az extrém nagy tranzakciós gráfból, hogyan lehet valamilyen alacsony dimenziós, a lehető legtöbb lényeges információt tartalmazó, véges időn belül kiszámolható érteket generálni.

A főkomponens-analízis alkalmas az információ ilyen jellegű tömörítésére. Ehhez azonban a gráf őrületes méretét le kell csökkenteni egy jól kezelhető méretre. Az első egyszerűsítés úgy tehető, hogy csak a hosszútávon aktív címeket használjuk, ezzel leszűrve a kiürült és nem használatos címeket. A második szűrés a gráf koncentráltabbá tétele. Ez úgy történik, hogy élünk egy feltételezéssel. Mégpedig azzal, hogy egy tranzakcióban szereplő bemeneti címek egy valós személyhez tartoznak és ezeket a címeket összehúzzuk egy csúcsba. Ezáltal egy olyan gráfot kapunk, amelyben egy él azt jelenti, hogy két személy között történt pénzutalás a vizsgált időszakban.

Így egy olyan gráfot kapunk, amely 1639 csúcsot tartalmaz 4333 éllel. Ez azon személyek összessége, akik a vizsgált 600 napos időtartamban legalább 100 tranzakcióban részt vettek.

A főkomponens-analízist pedig a következőképpen végezzük el. Vesszük minden nap ezen gráf állapotát és reprezentáljuk egy $n\ x\ n\ W(t)$ súlyozott szomszédsági mátrixszal, ahol az n a csúcsok száma és a súlyok a t-edik napon történt tranzakciók számai. $W(t)$ mátrixot átrendezzük egy l hosszú idősor vektorrá, ahol az l a gráf éleinek a száma. A vizsgált időszakra így kapunk egy $X = T\ x\ l$ gráf idősor mátrixot, ahol ennek a gráfnak a t-edik sora tartalmazza az l hosszú idősorát az adott napi tranzakciós mátrixnak. Az így kapott mátrixot soronként 1-re normálva már az elemzés szempontjából jól kezelhető mátrixot kapunk. Ezen a mátrixon szinguláris értékfelbontást végezve kaphatjuk meg az időfüggő főkomponenseket.

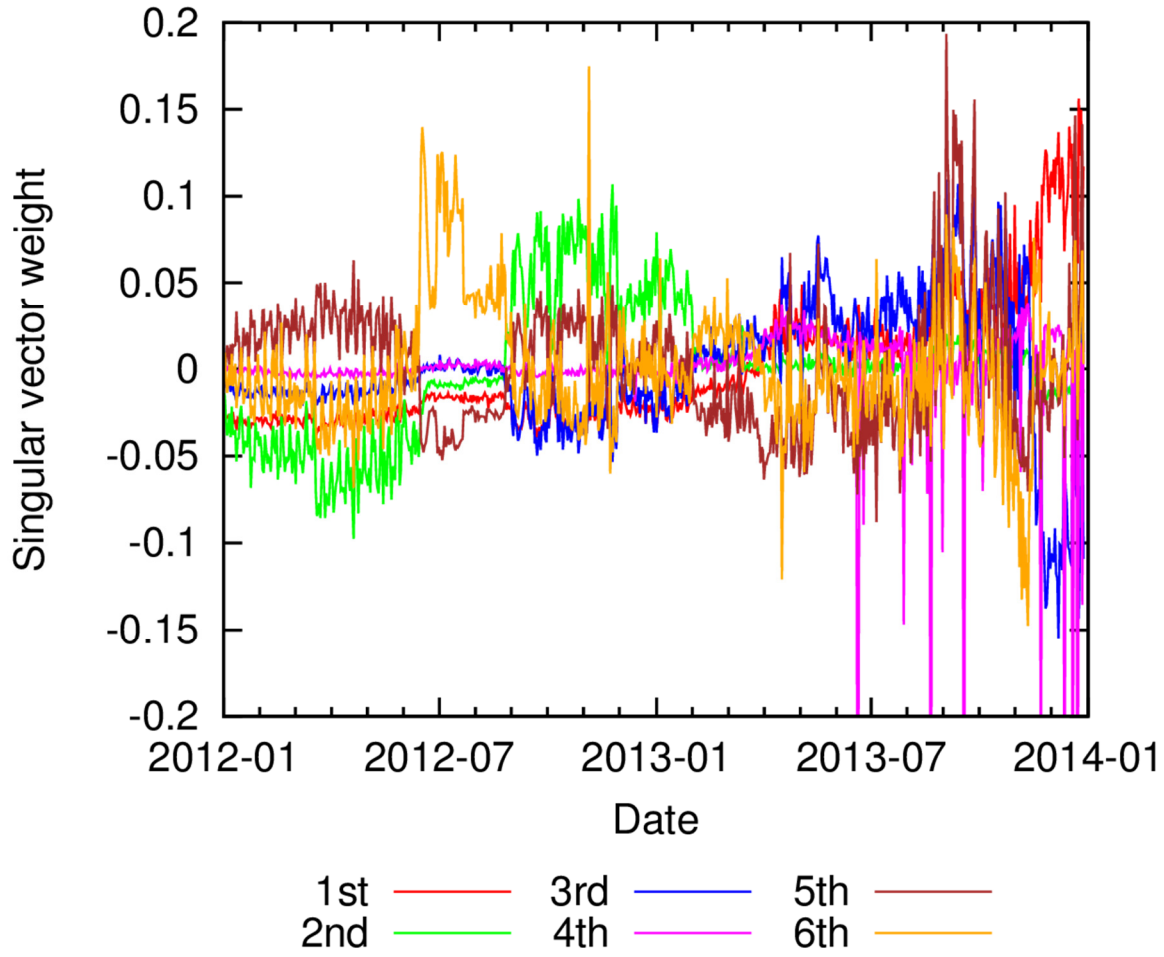
$$X = U\Sigma V^T$$

S egy diagonális mátrix, amely tartalmazza a szinguláris értékeket (S sajátértékeinek gyöke) az U és V^T pedig szinguláris vektorokat. Ezen mátrixok ortonormáltak, ezért a V^T-t tekinthetjük a hálózat bázisának. Szokás a szinguláris értékeket csökkenő sorrendbe tenni. Így a következő összefüggéssel tudjuk visszakapni az eredeti mátrixunkat:

$$x_{tj} = \sum_{i=1}^{T} \Sigma_{ii} u_j(t) v_{ji}$$

Az eredmények azt mutatják, hogy meglehetősen sok komponens szükséges a mátrix jó közelítésű visszakapására. Ebből arra lehet következtetni, hogy a rendszer sokdimenziós struktúrával rendelkezik és nem gaussos zajt is tartalmaz.

Főkomponensek



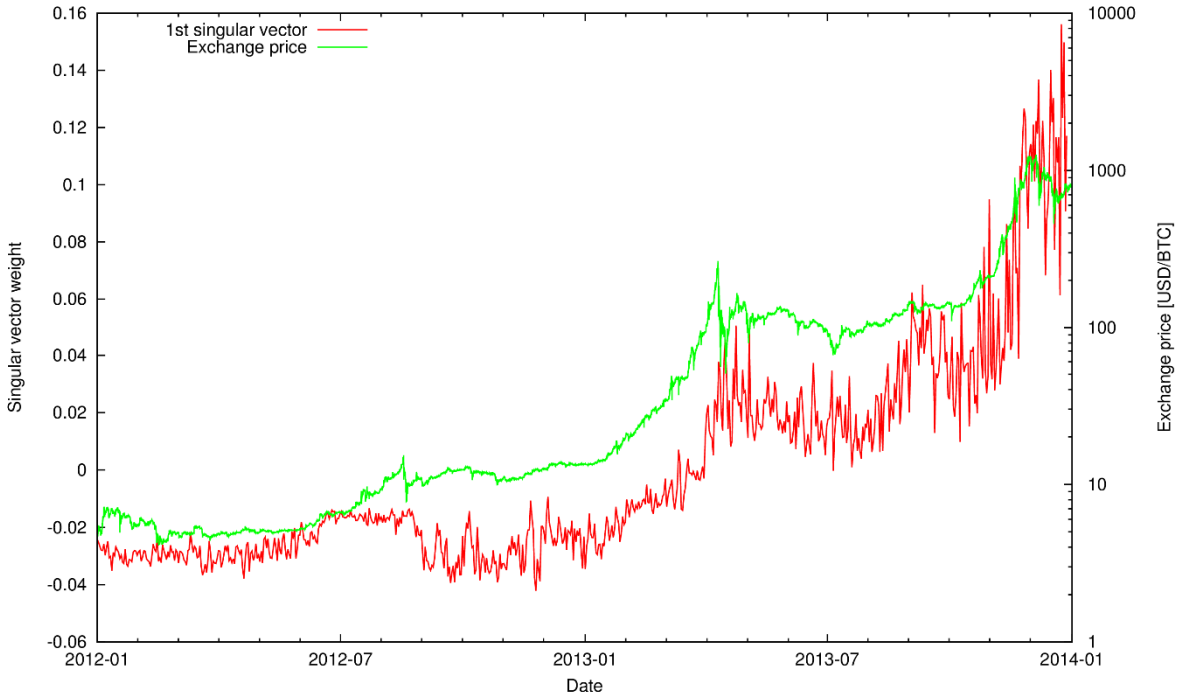
29. ábra

A 6 legnagyobb szinguláris értékkel rendelkező főkomponens az idő függvényében

Itt látható az első 6 $u_j(t)$ vektor. Látható, hogy időben jól azonosítható strukturális változásokon ment keresztül a hálózat. A tranzakciókat domináló szereplők lecserélődtek. Sajnos az anonimitás és az egy személyhez tartozó címek beazonosításának nehézsége miatt ezt nem tudjuk közvetlenül eseményekhez kötni.

Sokkal érdekesebb eredmény, hogy az első főkomponens erős korrelációban van az árfolyammal. Az alábbi ábrán látható a két idősor egyszerre, az árfolyam logaritmikus skálán.

Árfolyam és az első főkomponens



30. ábra

Az árfolyam és az első főkomponens az idő függvényében

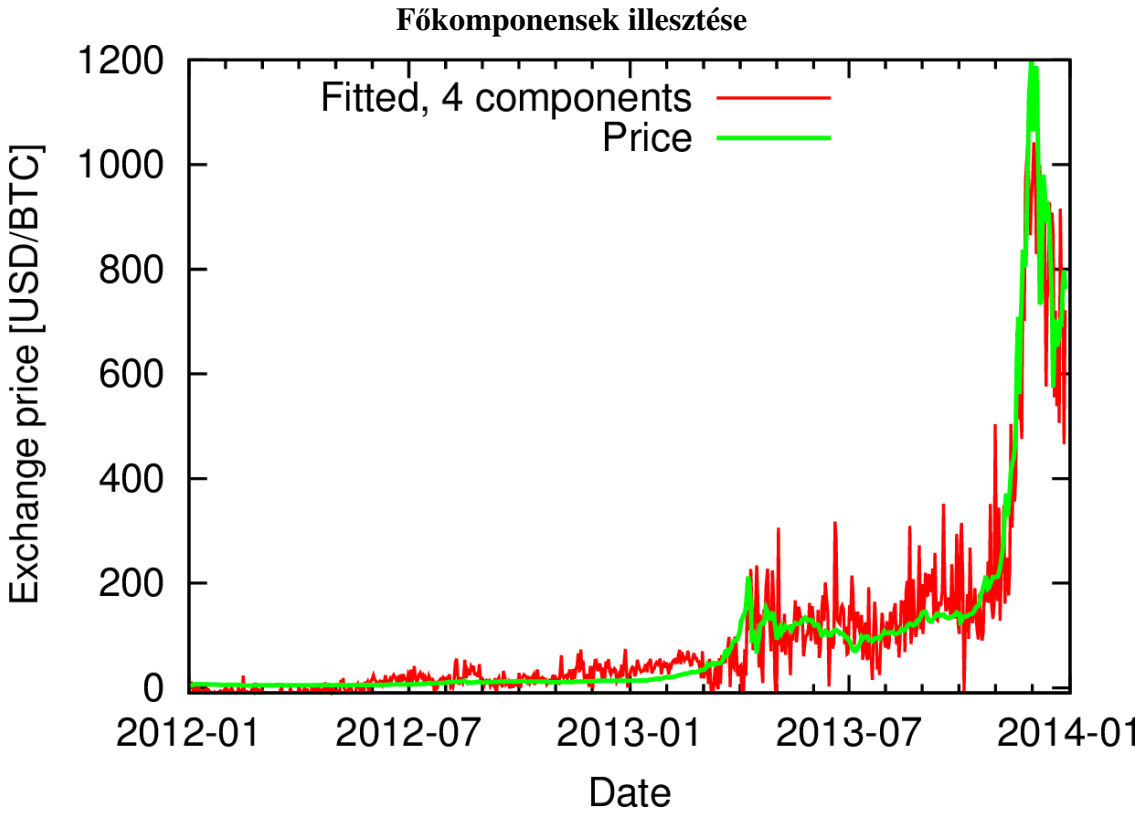
A korrelációk pedig a következők az első 5 főkomponens és az árfolyam között:

	Pearson korreláció	Spearman korreláció
1.	0.8528	0.865
2.	-0.033	0.436
3.	-0.378	0.44
4.	-0.074	0.591
5.	-0.0148	-0.299

Ha vesszük a lineárkombinációját a 4 legjobban korreláló főkomponens vektornak, akkor már elég jól rekonstruálható az árfolyamgörbe. Ez már szép eredménynek tekinthető. Azonban akkora hibát tartalmaz ez a fajta illesztési módszer, hogy közvetlenül nem lehet

eldönteni az ok okozati összefüggést a hálózat és az árfolyam között. Valamint rövid távú előrejelzést sem tudunk közvetlenül készíteni az árfolyamhoz a nagy fluktuáció miatt. Ezen az időskálán arra a következtetésre jutottunk, hogy gyakrabban előzi meg az árfolyamváltozás a hálózat mozgását. Ez nem jelenti, hogy a piac feltétlenül hatékony lenne, mert származhat a hiba az időskála hosszából, a gráfot koncentráló egyszerűsítő elv tökéletlenségéből és a szűrések okozta információveszteségből is.

Az alábbi ábrán látható az így illesztett árfolyamgörbe és az árfolyam az idő függvényében. Számomra igen meglepő eredmény, hogy ilyen pontossággal lekövetik egymást.



31. ábra

Az első négy főkomponensek lineárkombinációja és az árfolyam az idő függvényében

VII. Fejezet

A tranzakciós hálózat stressz tesztelése

Az eddigi vizsgálatok nagyon sok mindent megmutattak a bitcoin hálózat természetéről. Azonban arra a következtetésre jutottam, hogy ha kereskedési stratégiát akarok építeni az eddig megszerzett többlet információ alapján, akkor a hálózat vizsgált felbontása nem elég nagy. Adódik a kérdés, hogy ha feltételezem, hogy a bitcoin piac nem hatékony, akkor mennyi idő áll rendelkezésemre valamilyen piaci sokk esetében reagálni. Ez a hálózat szempontjából azt a kérdést veti fel, hogy milyen gyorsan terjed egy impulzus a tranzakciós hálózaton.

A hálózatok stressz tesztelésére gyakran alkalmazzák a biológiában gyakran használt vírusterjedési modellt az úgynevezett SIR (susceptible-infected-recovered) modellt. [21] Ez három különböző állapotba sorolja a gráf csúcsait: fertőzhető (S) , fertőzött (I) , már nem fertőzhető (R). A következő csatolt nem lineáris differenciál egyenletek megoldásával tudom időben nyomon követni e három csoportba tartozók számát.

$$\frac{dS}{dt} = -\frac{\beta SI}{N}$$

$$\frac{dI}{dt} = \frac{\beta SI}{N} - \gamma I$$

$$\frac{dR}{dt} = \gamma I$$

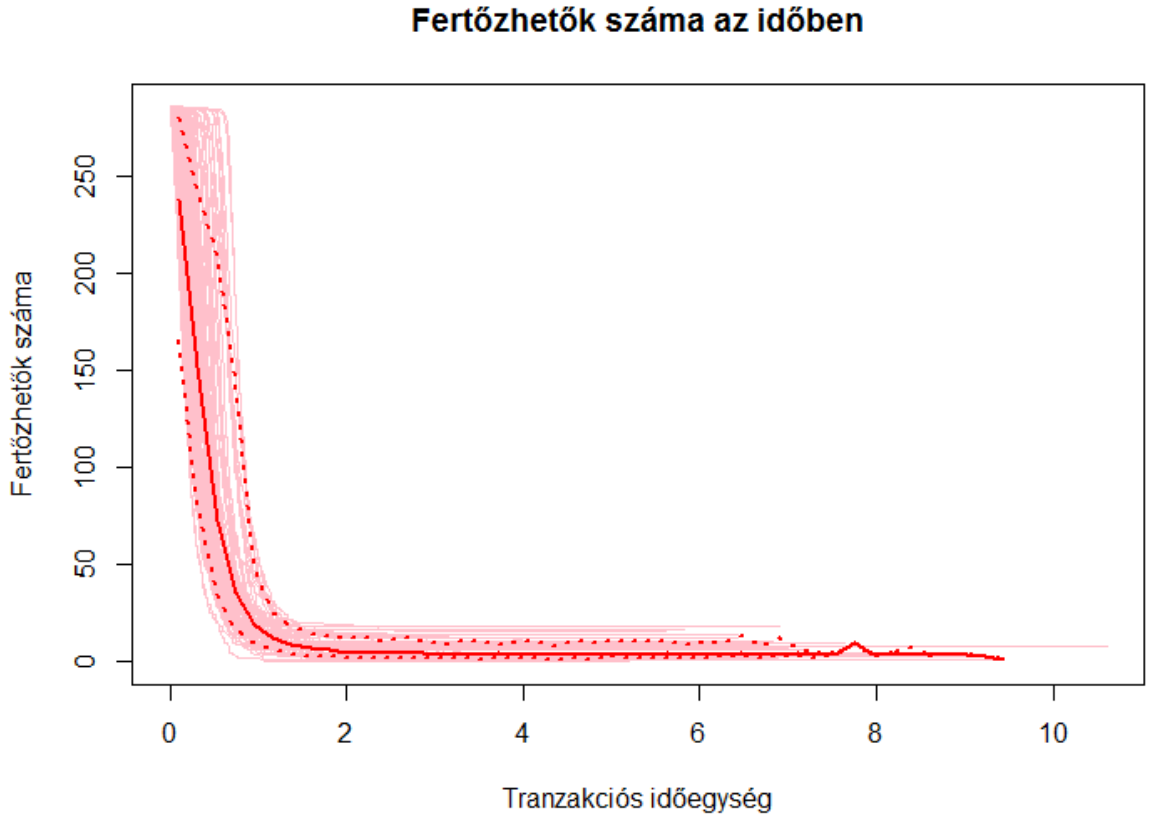
$$S(t) + I(t) + R(t) = N$$

A két paraméter amellyel szabályozni tudom a „fertőzés” és „gyógyulás” mértékét a β és γ, amelyek pozitív számok.

A modellt a tranzakciós hálózatban csak annyiban kell módosítani, hogy a fertőzés nem terjedhet bármilyen irányba, csak az összekötött csúcsok között. A szimuláció tehát a következő módon próbálja modellezni egy pánik szituációját. A negatív információ bejut valamilyen ponton a rendszerbe és a rendszer tagjai szeretnének megszabadulni a bitcoinoktól, ezért tranzakciókat kezdeményeznek a hálózaton: Aki az S halmazba tartozik még nem szabadult

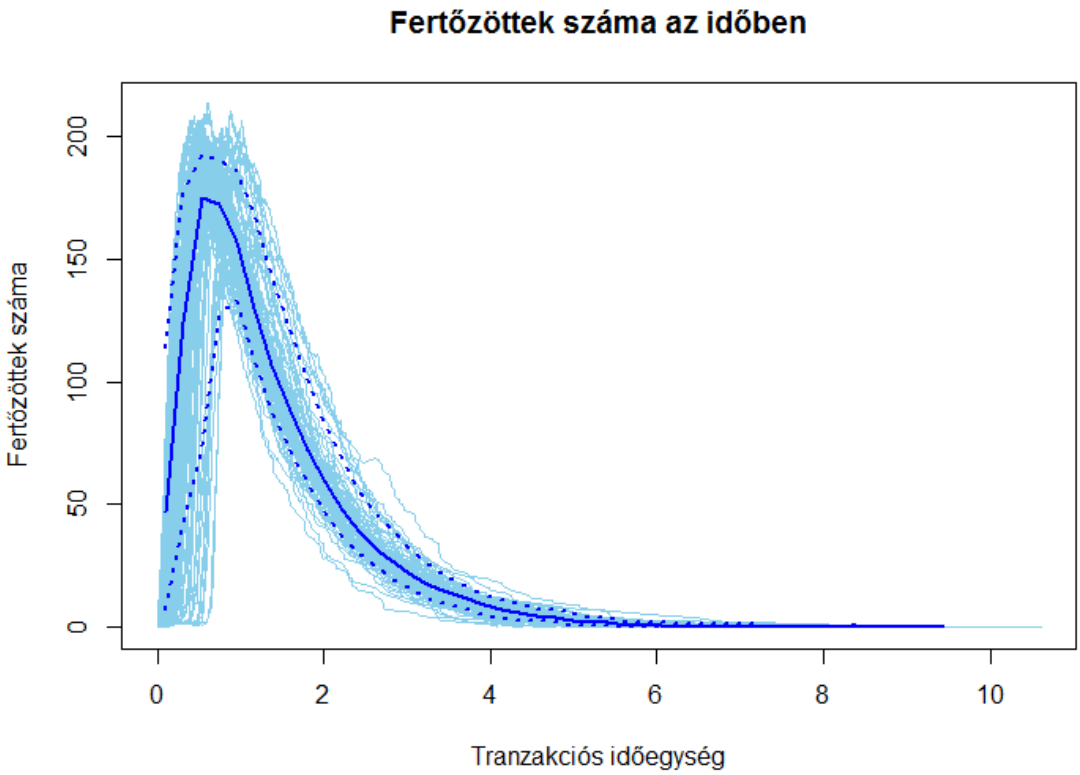
meg a bitcoinjától, aki I-be, már tovább utalta valahova, de az ő címzettje is tovább akarja még utalni. Az R-be képzeljük mindazokat a személyeket, akik nem akarnak már megszabadulni a bitcoinjaiktól. Ebben az esetben a β a pánik erősségét méri, a γ pedig annak a mértékét,hogy hány tranzakción keresztül jut el valamilyen nyugvó állapotba (valamilyen tőzsde számlájára például) a bitcoin. Ezeknek a beállítására az eredeti biológiai modellben mérési lehetőségek vannak az ismert fertőző kórokozókra vonatkozóan, itt azonban elméleti megfontolásból nehéz ezeket a paramétereket megadni. A számítási kapacitást figyelembe véve ezért egy olyan széles skálán vizsgálom ezeket a paramétereket amennyire csak lehetséges.

A karakterisztikus időnek azt az időtartamot tekintem, amikor a szereplők 99%-a megszabadult azoktól a bitcoinoktól, amiktől akart. Egy adott paraméterrel a szimuláció százszor futott le és a következő ábrákon látható egy ilyen szimulációnak az $S(t)$, $I(t)$,és $R(t)$ függvénye (ezekben az esetekben β = γ =1).

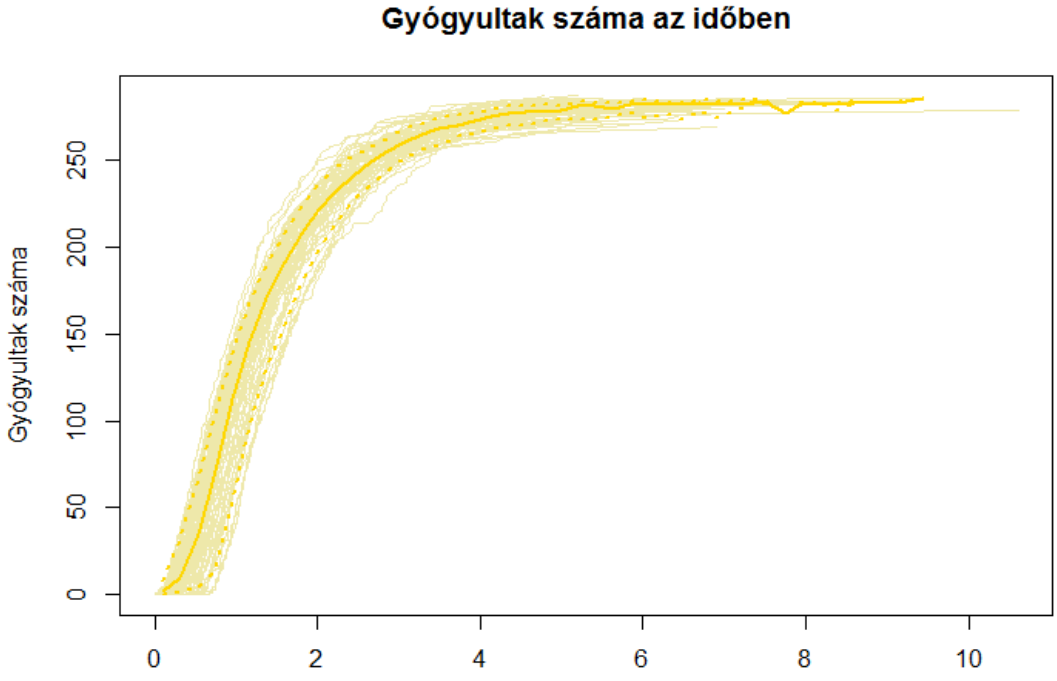


32. ábra

A bitcointól szabadulni akaró felhasználók száma az időegység függvényében



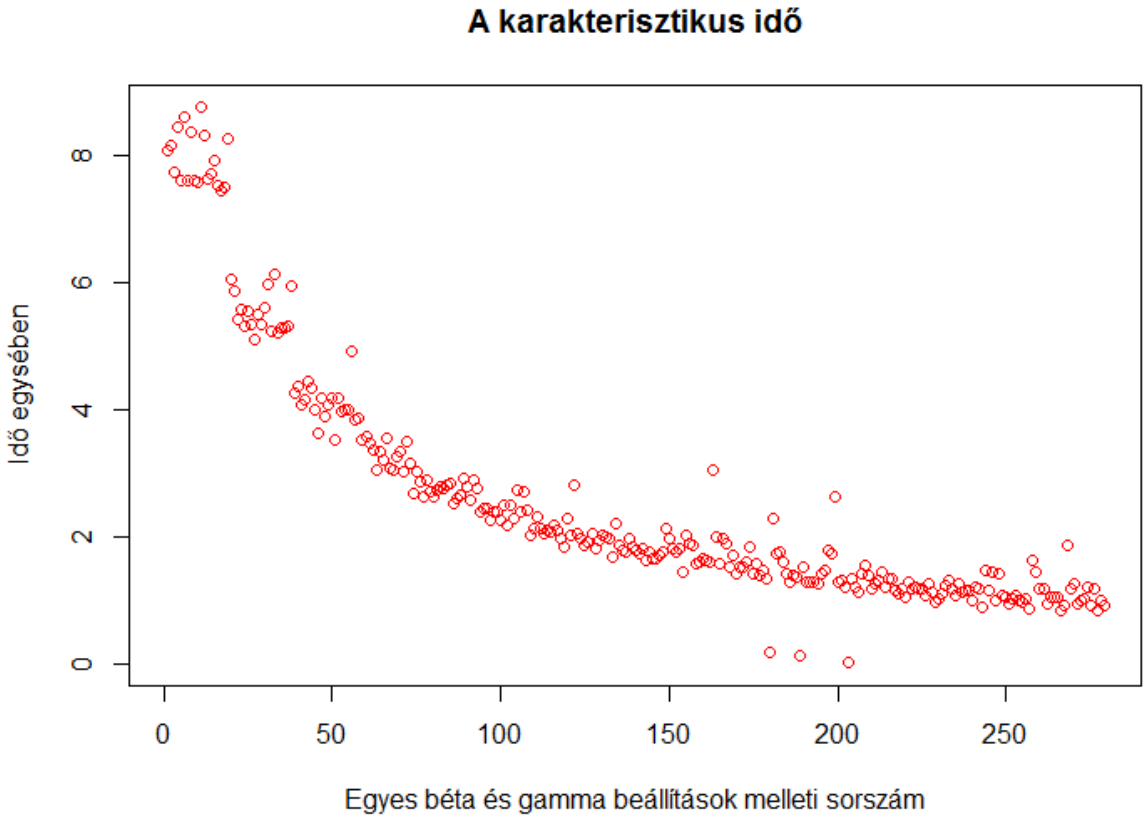
33. ábra
A bitcointól szabaduló felhasználók száma az időegység függvényében



34. ábra
A bitcointól már szabadulni nem akaró felhasználók száma az időegység függvényében

A szimulációk azt mutatják, hogy a két paratmétert 0.5 és 5 között érdemes megválasztani. Ha ennél kisebb értékkel próbálkozom, akkor a legtöbb esetben az impulzus végig sem fut a hálózaton, nagyobb érték esetében pedig olyan gyorsan bekonvergál az 1 időegységbe a folyamat, hogy egészen biztosan nem valós szituációt modellezek vele.

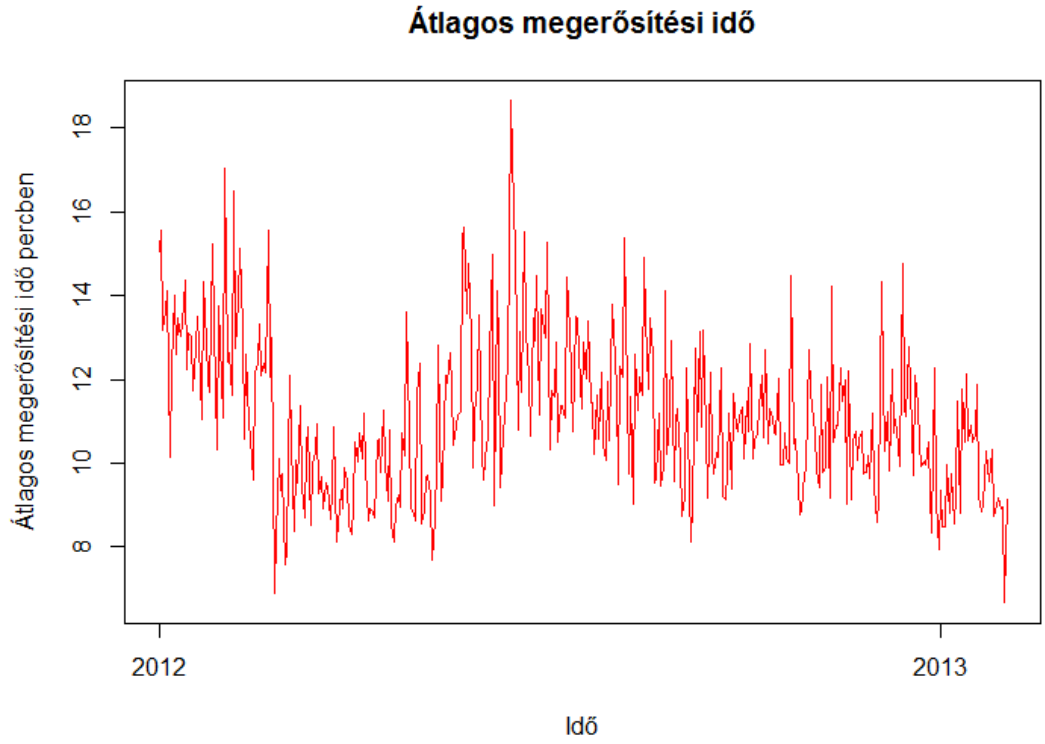
A következő ábrán láthatjuk [0.5, 5] intervallumon egyenletes lépésekkel haladva 279 féle különböző paraméterpárral lefuttatott szimulációk karakterisztikus idejét (egy pont egy paraméterpárral 100 szimulációt jelent).



35. ábra
A pánik karakterisztikus ideje időegységben a különböző bementi paraméterpárok növekvő sorrendjének függvényében

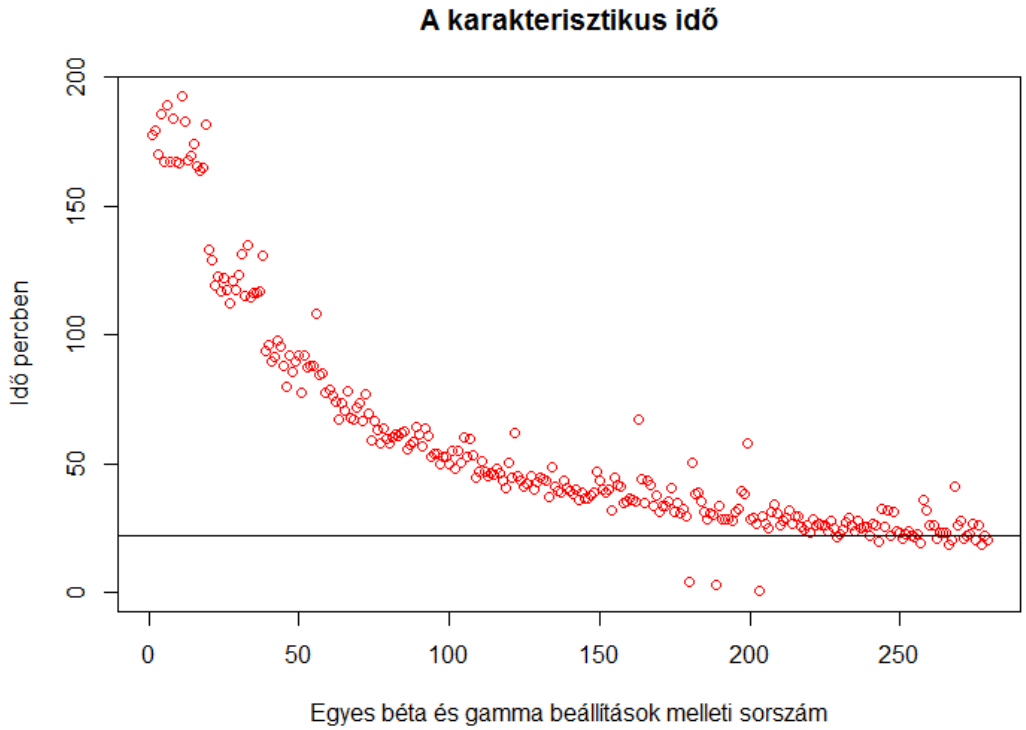
Hogy milyen valós időt feleltetek meg ennek a karakterisztikus időnek, az nehéz kérdés. Az egyes bitcoin tőzsdéken a ki- és beutalás hitelességét a tranzakció megerősítési számával mérik. A megerősítési számot az adott tranzakció blokkjára épülő újabb blokkok számából számolja a rendszer. Egy átlagos bitcoin tőzsde 2-3 megerősítést vár meg mielőtt elismeri, hogy valóban hiteles a ki- és beutalás.

A vizsgált időszakban a következő ábra mutatja egy megerősítés érkezésének napi átlagos idejét.



36. ábra
Az átlagos megerősítési idő az idő függvényében

Ennek a görbének az átlaga 11 perc, tehát két megerősítéshez körülbelül 22 perc időre van szükség. Ez alapján azzal a közelítéssel élek, hogy a hálózaton a karakterisztikus idő egysége ebbe a nagyságrendbe esik. Nézzük meg újra az ábrát most már percben mérve.



37. ábra

A pánik karakterisztikus ideje percben a különböző bementi paraméterpárok növekvő sorrendjének függvényében

Ez alapján azt mondhatom, hogy egy nagyobb jelentőségű esemény esetén körülbelül órás nagyságrend az az idő, ami alatt a hálózat azt lereagálhatja. Ez alapján nem meglepő, hogy nem tudtunk ok okozati kapcsolatot felfedezni az árfolyam és a hálózat nagyskálás szerkezete között.

VII. .Fejezet

Kereskedés bitcoinnal

Az eddigi vizsgálatok eredményei arra sarkalltak, hogy egy olyan szoftver írásába kezdjek, amely valós időben tud adatokat feldolgozni és automatikusan kereskedni a bitcoin tőzsdéken.

Erre azért van lehetőség, mert a bitcoin tőzsdékre minimális tőkével is ki lehet lépni és a minimális tranzakciók mérete is alacsony (600 forint környékén van). Regisztráltam magam a három legnagyobb bitcoin tőzsdén és a BTC-e.com-ra optimalizálva elkészítettem egy alapkereskedő Python kódot, amely a következő parancsokra képes:

- lekéri az egyenleget
- lekéri az aktív bid offer ajánlatokat
- bid vagy offer ajánlatot tesz adott árfolyam és mennyiség mellett
- lekéri az elmúlt x tranzakciót, a napi maximumot, minimumot
- lekéri a saját teljesült kereskedéseket
- lekér bármilyen adatot a blockchainből

Bármilyen parancsot 1 percenként tud ismételni automatikusan. A másik lehetőség, hogy a hét bármely napján akármilyen időpontot beállíthatok a parancs automatikus elvégzéséhez.

Sajnos kereskedési jogosultságom a dolgozat megírásának pillanatában még a másik két bitcoin tőzsdén nincsen, mert egy azonosítási procedúrán részt kell vennem.

A karakterisztikus időt figyelembe véve egy olyan stratégiában látok pozitív hozamra lehetőséget, amely a három tőzsdén figyeli az árfolyam és bid offer ajánlatok mozgását, megtámogatva a nagyobb bitcoin tranzakciók figyelésével a hálózaton. Arra alapozva, hogy a három tőzsdén az átlagos kereskedési kedv a felhasználók különböző földrajzi elhelyezkedése révén más egy adott időpillanatban (míg a BTC-e Európai nappalkor aktív, a btcChina ázsiai nappalkor, míg a Bitstamp EST időzóna szerint) arra számítok, hogy a karakterisztikus idő nagyságrendjében még van különbség az egyes bitcoin tőzsdéken jegyzett árak között és fel lehet egy olyan piaci pozíciót venni, amely ezt kihasználja.

Összefoglalás

Az eredményekből azt a végkövetkeztetés tudom levonni, hogy más, fizikai, biológiai, gráfelméleti és informatikai területeken használatos modellek és adatbányászati módszerek alkalmazása a bitcoin hálózat feldolgozására is használható. Mára technikailag is megvalósítható ekkora számítás- és tárolásigényes hálózatok és adatbázisok kezelése. Bitcoin mint fizetőeszköz még nem terjedt el igazán, lehet nem is fog. A vizsgálatokat azonban véleményem szerint nem szabad abbahagyni, sőt érdemes lehet ezen területre a továbbiakban még jobban odafigyelni, mert lehetséges, hogy egyszer a jövőben mindennapjaink részévé válnak a bitcoin elvű tranzakciók.

A téma általam történt, lehetőségeim szerint legátfogóbb elemzése és kutatócsoportunk eredményei tükrözik a bitcoin hálózat vizsgálatának széleskörű lehetőségeit. Remélem, felkelti az Olvasó érdeklődését, és látható a dolgozatban, hogy milyen jövőt befolyásoló kutatási terület lehet ez a téma. Számomra meglepetést okozott jó pár kutatási eredmény, a bitcoin tranzakciós elvet rendszerszemlélettel vizsgálva úgy érzem, a pénzügyi világ sok területen alkalmazhatná a pénzügyi tranzakciók felgyorsítása érdekében. Dolgozatomban szerettem volna felhívni az interdiszciplinaritás fontosságára a figyelmet, hogy mennyi tudományterület eredményeit lehet egy új területen alkalmazni.

A témával való foglalatoskodásomat ezzel a dolgozattal nem szeretném lezárni.

Irodalomjegyzék

[1] S. Nakamoto, „Bitcoin: A peer-to-peer electronic,” http://bitcoin.org/bitcoin.pdf, 2008.

[2] P. Mileff, „P2P hálózatok,” Miskolci Egyetem Általános Informatikai Tanszék, 2009.

[3] C. Dwork és M. Naor, „Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology,”

Lecture Notes in Computer Science, %1. szám750, p. 139–147, 1993.

[4] „Protocol documentation,” 02 2015. [Online]. Available: https://en.bitcoin.it/wiki/Protocol_documentation.

[5] D. Szabó, „BITCOIN FUNDAMENTÁLIS ELEMZÉS,” [Online].

Available: http://superposition.hu/hu/blog/bitcoin-fundamentalis-elemzes.

[6] F. N. David, Games, Gods, and Gambling: A History of Probability and Statistical Ideas, Courier Dover Publications, 1998.

[7] „History of bitcoin,” [Online]. Available: https://en.bitcoin.it/wiki/History.

[8] „Blockchain,” [Online]. Available: http://blockexplorer.com/block/000000000019d6689c085ae16

5831e934ff763ae46a2a6c172b3f1b60a8ce26f.

[9] „Bitcoin Price Chart with Historic Events,” [Online]. Available: https://bitcoinhelp.net/know/more/price-chart-history.

[10] „Blockchain,” 2015. [Online]. Available: blockchain.info.

[11] R. Graham és M. Grötschel, Handbook of combinatorics, Elsevier, 1995.

[12] R. Albert és A.-L. Barabasi, „Statistical mechanics of complex networks,” *Reviews of Modern Physics,* 2002.

[13] R. Dorfman, „Formula for the Gini Coeffcient,” *The Review of Economics and Statistics,* 1979.

[14] A.-L. Barabási és R. Albert, „Emergence of scaling in random networks,” *Science,* 1999.

[15] D. Kondor, M. Pósfai, I. Csabai és G. Vattay, „Do the rich get richer? An empirical analysis of the BitCoin transaction network,” *PLoS ONE,* 2014.

[16] J. Menche, A. Valleriani és R. Lipowsky, „Asymptotic properties of degree-correlated scale-free net,” *PHYSICAL REVIEW E,* 2010.

[17] M. E. J. Newman, „Clustering and preferential attachment in growing networks,” *Physical Review E,* 2001.

[18] O. S. Klass, O. Biham, M. Levy, O. Malcai és S. Soloman, „The Forbes 400 and the Pareto wealth distribution,” *Economics Letters,* 2006.

[19] R. K. Merton, „The Matthew Effect in Science,” *Science,* 1968.

[20] D. Kondor, I. Csabai, J. Szüle, M. Pósfai és G. Vattay, „Inferring the interplay between network structure and market effects in Bitcoin,” *New Journal of Physics,* 2014.

[21] N. F. Britton, Essential Mathematical Biology, Springer, 2003.

[22] „Szolgáltatásmegtagadással járó támadás,” [Online]. Available: http://hu.wikipedia.org/wiki/Szolgáltatásmegtagadással_járó_támadás.

NYILATKOZAT

Név: Bakó Tamás

ELTE Természettudományi Kar, szak: Biztosítási és pénzügyi matematika MSc

NEPTUN azonosító: RD8KDP

Szakdolgozat címe:

Bitcoin hálózatok elemzése

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló munkám eredménye, saját szellemi termékem, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2015.05.04.

_____

a hallgató aláírása