A Bitcoin tranzakcióhálózat fejlődésének vizsgálata adatbányász módszerekkel

Kondor Dániel
ELTE, Komplex Rendszerek Fizikája Tanszék

MAFIHE Téli Iskola
2015 február 4

Bitcoin, alapok

- Teljesen elosztott pénzügyi rendszer
- Nincs központi hatóság, bárki csatlakozhat
- Tranzakciók listája nyilvános
- Felhasználók nem azonosíthatóak könnyen
- Biztonság: peer-to-peer hálózat közös munkája alapján

Bitcoin, rövid történet

Feltaláló: Satoshi Nakamoto (álnév?), 2008

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin, rövid történet

01
DEC / 2013

Satoshi Nakamoto is (probably) Nick Szabo

I recently became interested in identifying the pseudonymous creator of Bitcoin, Satoshi Nakamoto. I started from the Bitcoin whitepaper [0] published in late 2008, and proceeded to run reverse textual analysis – essentially, searching the internet for highly unusual turns of phrase and vocabulary patterns (in particular places which you would expect a cryptography researcher to contribute to), then evaluating the fitness of each match found by running textual similarity metrics on several pages of their writing.

Which led me rather directly to several articles from Nick Szabo's blog.

https://likeinamirror.wordpress.com/

Bitcoin, rövid történet

- Első blokk: 2009. január
- Nagy érdeklődés 2011 óta
- Növekedés: árfolyam: 2000x 3 év alatt, bányászás nehézsége: 40 milliárd 6 év alatt
- Bitcoin bányászok összes számítási teljesítménye: világ legerősebb szuperszámítógépe x 100 ezer

Bitcoin, felhasználhatóság

Overstock.com - Probably the biggest retailer that accepts Bitcoin
Wordpress - The popular blogging platform used by some of the biggest media companies in the world, including The New York Times, CNN, Reuters, Mashable, NBC Sports, GigaOm, and TechCrunch, started accepting Bitcoins in November 2012.
The Pirate Bay - One of the biggest BitTorrent directories on the Net
Reddit - Reddit allows users to purchase Reddit Gold using Bitcoins, a feature they added back in February 2013.
Virgin Galactic - The Richard Branson-led aviation company started accepting Bitcoin for customers who are interested in flying to space and paying for it using Bitcoin.
OkCupid - The online dating site started accepting Bitcoin for premium services.
Zynga - The popular mobile gaming company.
PayPal
eBay
Tesla

Read more: http://www.nasdaq.com/article/what-companies-accept-bitcoin-cm323438#ixzz3LVcXAhxv

Figure 4: The physical items we purchased with bitcoins, including silver quarters from Coinabul, coffee from Bitcoin Coffee, and a used Boston CD from Bitmit. The items in green were purchased from CoinDL; in blue from Bitmit; and in red using the payment gateway BitPay.

Bitcoin, alapok

Transaction View information about a bitcoin transaction

50c28ab704710429c26ccb082303f32b6873362ada4b596ab8b6b721df4ae2e8

17ux9YmBEiXfVX47fVkAHyDLLNY9n2DkdD 1HCmhcepXYPEC9j8StYVDkHJsfUotXhqEw	1D82PmjdqCvp8UckacX82BW9NdSanGs2X	107 BTC
	12CqiZisMYhnPFaT86LaRWCsvB3Licxdzi	43.2500001 BTC
	1Jgmf8qHBEjC2LTBSVd6KMtohxiGAvbAcG	43.2500001 BTC
	1J9U9YYv3hBzJdoivgDbyjVqpM5MZf2iwh	43.2500001 BTC
	1P5zutJb7fPVjMcNB26no8uBENELncipMJ	43.2499997 BTC
	14JvPzPKruEDEgHcWmuar1wCbavPcFS6sX	0.00589455 BTC

Unconfirmed Transaction! 280.00589455 BTC

Summary	
Size	575 (bytes)
Received Time	2013-09-19 11:58:57
Estimated Confirmation Time	9 minutes (queue position 218)
Relayed by IP	Blockchain.info
Visualize	View Tree Chart

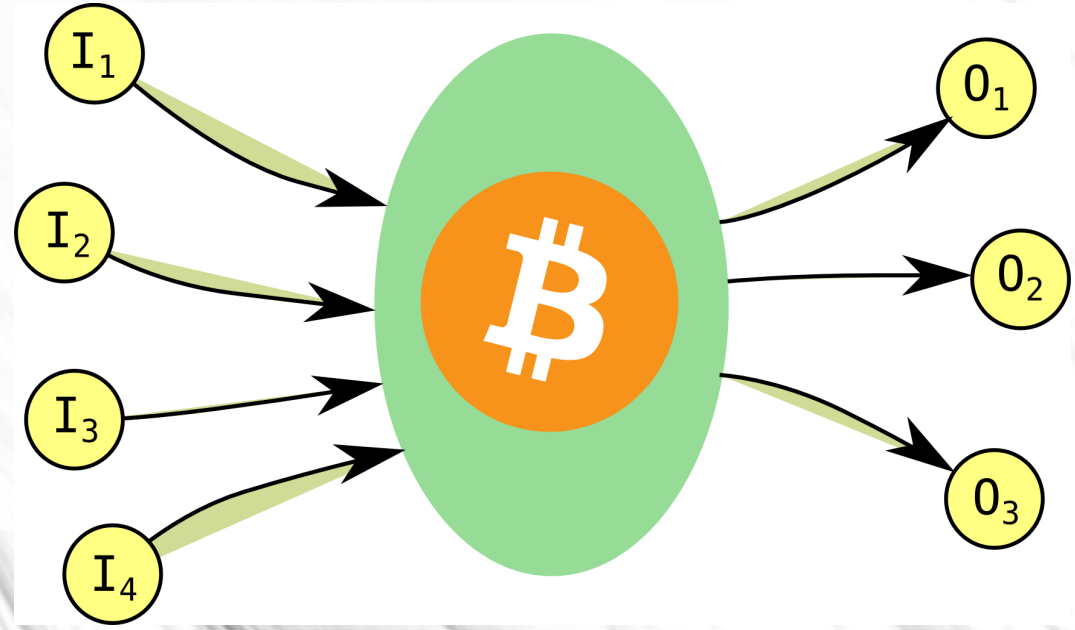
Inputs and Outputs	
Total Input	280.00639455 BTC
Total Output	280.00589455 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	280.00589455 BTC
Scripts	Show scripts & coinbase

blockchain.info

Bitcoin, alapok

Két kihívás:

- Címekhez tartozó összeg védelme: csak az tudja elkölteni, akihez tartozik
- Csalás elleni védelem: ne lehessen többet költeni, mint amennyivel valaki rendelkezik



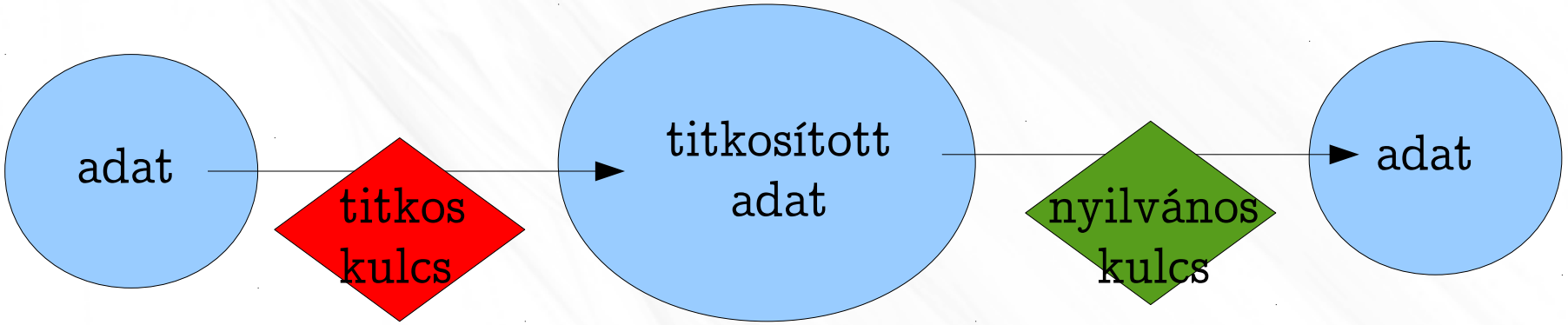
Bitcoin, megvalósítás

- Minden tranzakció bemenete egy korábbi tranzakció kimenetére kell, hogy hivatkozzon
- Lopás elleni védelem: kimenetben “feldadvány”, amit csak az igazi címzett tud “megoldani”, ez kell az elköltéshez
- Csalás elleni védelem: ha több tranzakció akarja ugyanazt a kimenetet elkölteni, akkor csak egyet fogadunk el $\leftrightarrow$ ehhez kell: résztvevők meg kell egyezzenek, hogy melyiket!

Bitcoin, megvalósítás

Lopás elleni védelem: nyilvános kulcs titkosítás (public key cryptography)

$\rightarrow$ minden Bitcoin cím igazából egy kulcspár, a tranzakciókat a titkos kulccsal kell aláírni, a nyilvános kulccsal lehet ellenőrizni



Titkosítás

$f_1(A,K_1) = B$ $f_2(B,K_2) = A$ nem invertálhatóak

$K_1 = K_2$ szimmetrikus

“legegyszerűbb”: $f_1 = f_2 = XOR$, $K_1 = K_2$

K_1 != K_2 asszimmetrikus, ekkor:

K_1 titkos kulcs

K_2 nyilvános kulcs

Bitcoin tranzakció

- Tranzakció kimenete: nyilvános kulcs (cél cím) + “adat”
- Következő tranzakció bemenete: hivatkozás az előző kimenetre + “adat” a titkos kulccsal titkosítva

$\rightarrow$ ez biztosítja, hogy csak az tudja elkölteni, aki arra tényleg jogosult

Csalás elleni védelem

- Tfh. két “érvényes” tranzakció, ami ugyanazt az összeget költi el
- Kérdés: melyiket fogadjuk el? Hálózat résztvevői között egyetértésnek kell lennie.
- Megoldás: “bányászás”, blockchain

Bitcoin, blokkok

- Egy blokk: valahány tranzakció összegyűjtve + időbélyeg + előző blokk azonosítója + szabadon változtatható paraméter
- Szabály: hash-fv. a blokk adataira legyen egy küszöb alatt
- Bárki próbálkozhat így blokkot létrehozni
- Akinek sikerül, kap 25 (eredetileg 50) bitcoint
- A küszöbszint az összes számítási kapacitás függvényében változik

Hash függvények

- f(A) = B
- A n-bit, B m-bit, általában m < n
- B egyenletes eloszlású (olyan, mintha véletlen lenne); ez függ persze A eloszlásától
- Nem invertálható (csak nehezen), kis változás A-ban → nagy változás B-ben
- Példa: Pearson's hash:
  h = (h+d[i])%256; h = x[h]
- Felhasználás: checksum, titkosítás, adattárolás

Bitcoin, blockchain

- Egy új blokk kiszámítása “nehéz”, csak próbálgatással lehet (“bányászás”)
- Ha a blokk generálója betartja a szabályokat, akkor a duplán elköltött tranzakciókból csak az egyiket veszi bele, az lesz a “kanonikus”
- Blokkok egymásra épülnek, később megváltoztatni csak az összes blokk újraszámolásával lehet
- Ha a bányászok többsége tisztességes, akkor nem lehet csalni

Bitcoin, blockchain

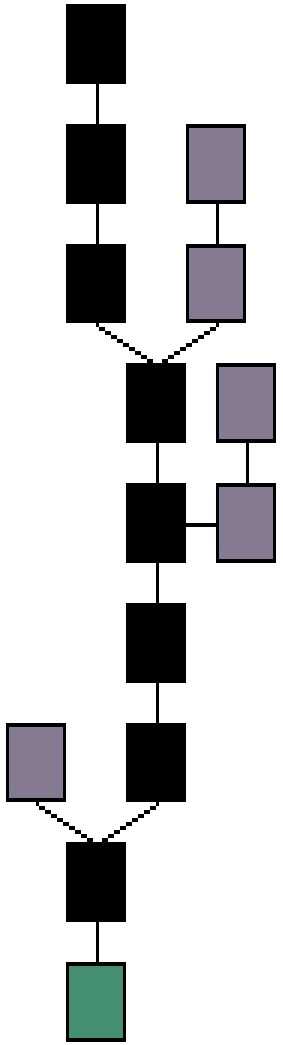
Blockchain Home Charts Stats Markets Developers Wallet

Block #258832

Summary	
Number Of Transactions	117
Output Total	3,670.87012748 BTC
Estimated Transaction Volume	1,747.23522626 BTC
Transaction Fees	0.05791943 BTC
Height	258832 (Main Chain)
Timestamp	2013-09-19 11:25:48
Received Time	2013-09-19 11:26:00
Relayed By	ASICMiner
Difficulty	112,628,548.67
Bits	421929506
Size	45.298828125 KB
Version	2
Nonce	2997094945
Block Reward	25 BTC

Hashes	
Hash	000000000000000cf9c799921f03073efbf8f40cd358a39b33d3bf36cb6b02e8
Previous Block	0000000000000016dbf3752370945380c846c490348d130399263029c64ab8eb
Next Block(s)	00000000000000002137263c054025a8a0f3f0d7ce7dac5a85cf6f7f40f243af5c
Merkle Root	0940aa86faec11aa81454badf9b01e705f9e6461f9204c9835ce58b4605ed563

Network Propagation (Click To View)



Bitcoin, adatok

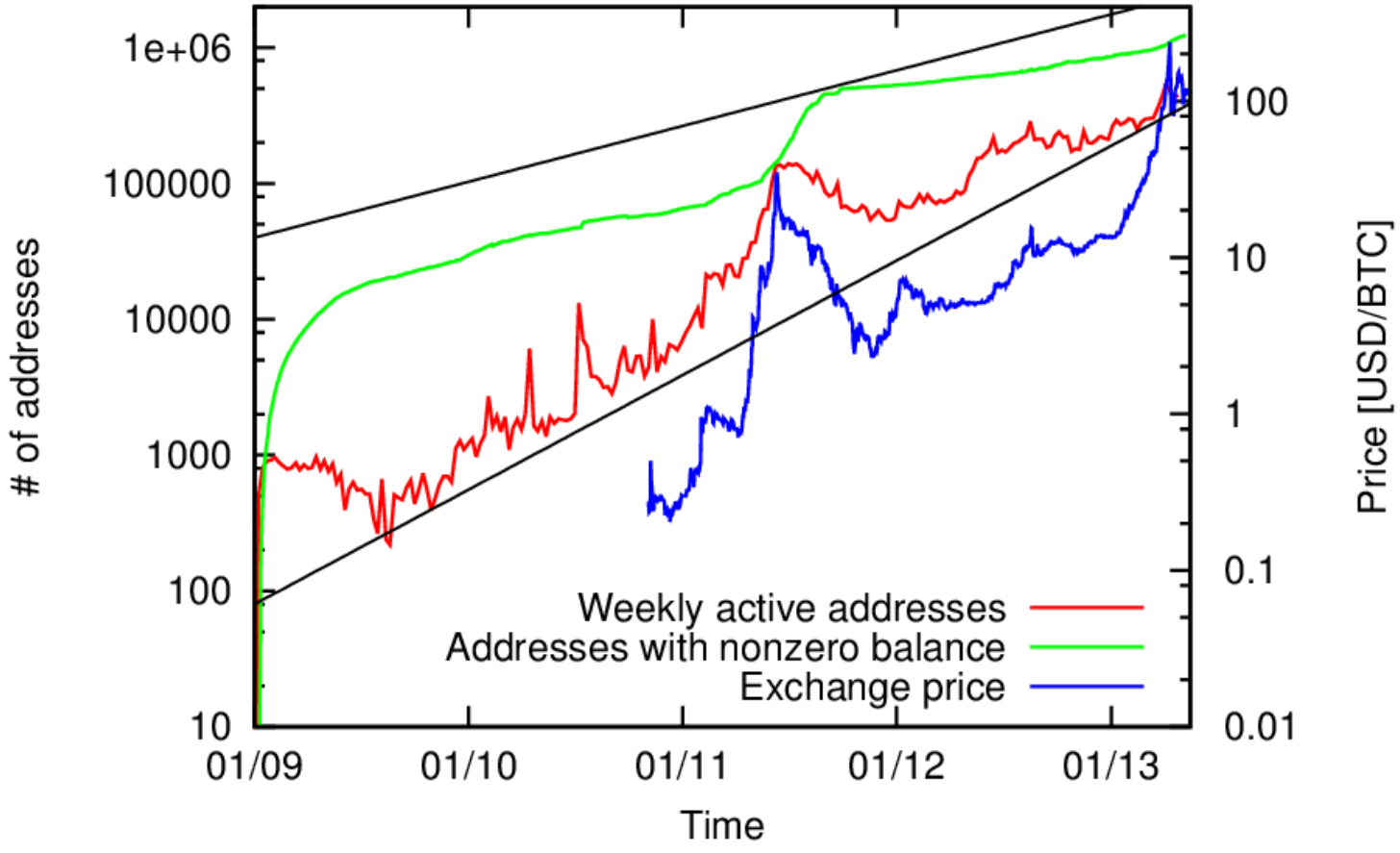
- Több nyílt forráskódú kliens elérhető
- Mi a bitcoind általunk módosított változatát használjuk
- A kliens automatikusan csatlakozik és letölti az adatokat
- Módosítás: adatok kiírása szöveges fájlokba

Bitcoin, adatok

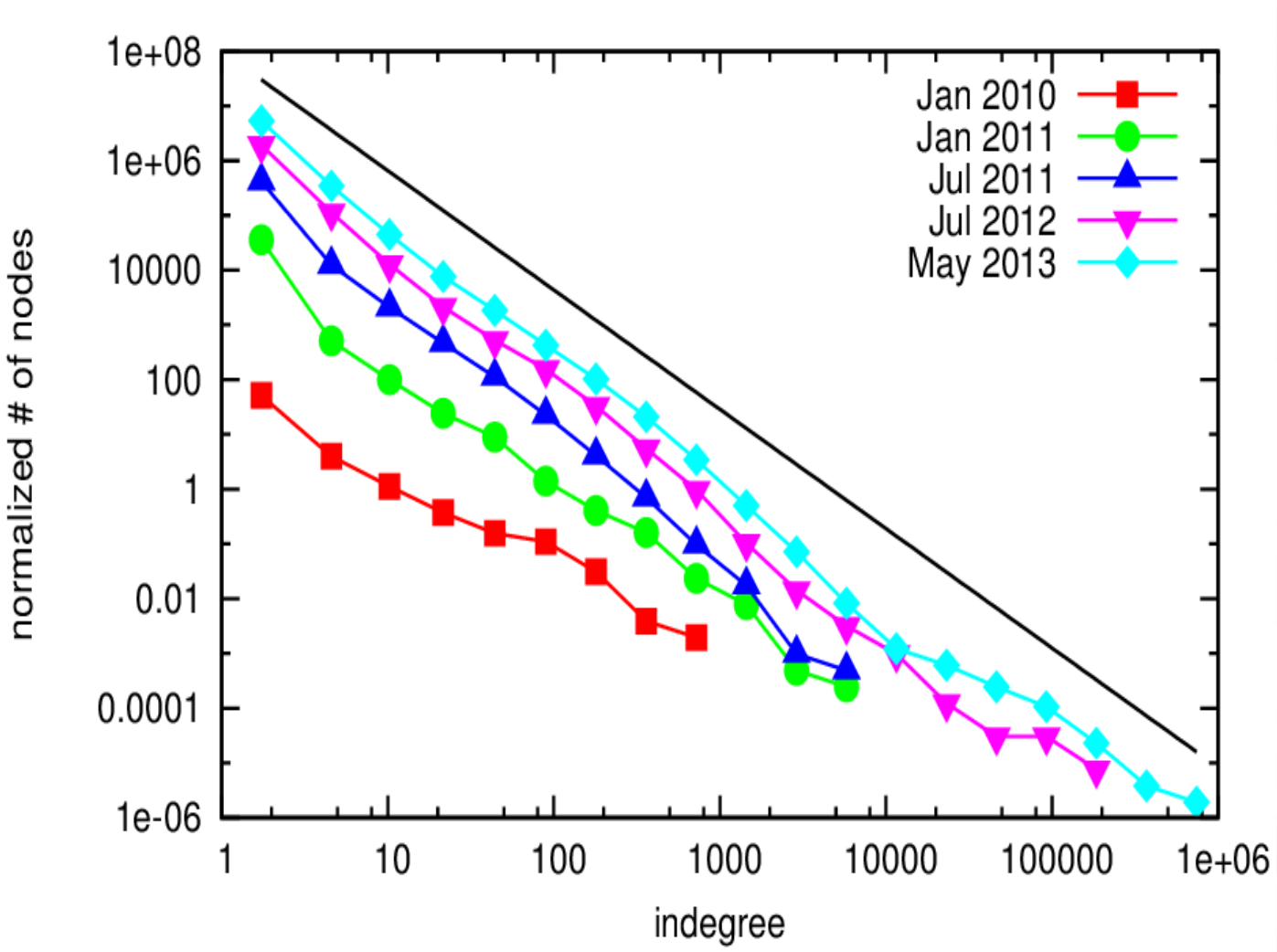
- Összes tranzakció
- Bemenetek és kimenetek felsorolása
- Bitcoin címek, összegek
- Időpontok a blokkokhoz
- Tárolás: adatbázisszerver
- Extra feladat: címek összerendelése felhasználókhoz

Bitcoin, statisztikák

- Alapvető statisztikák könnyen számolhatóak az adatbázisunkon belül

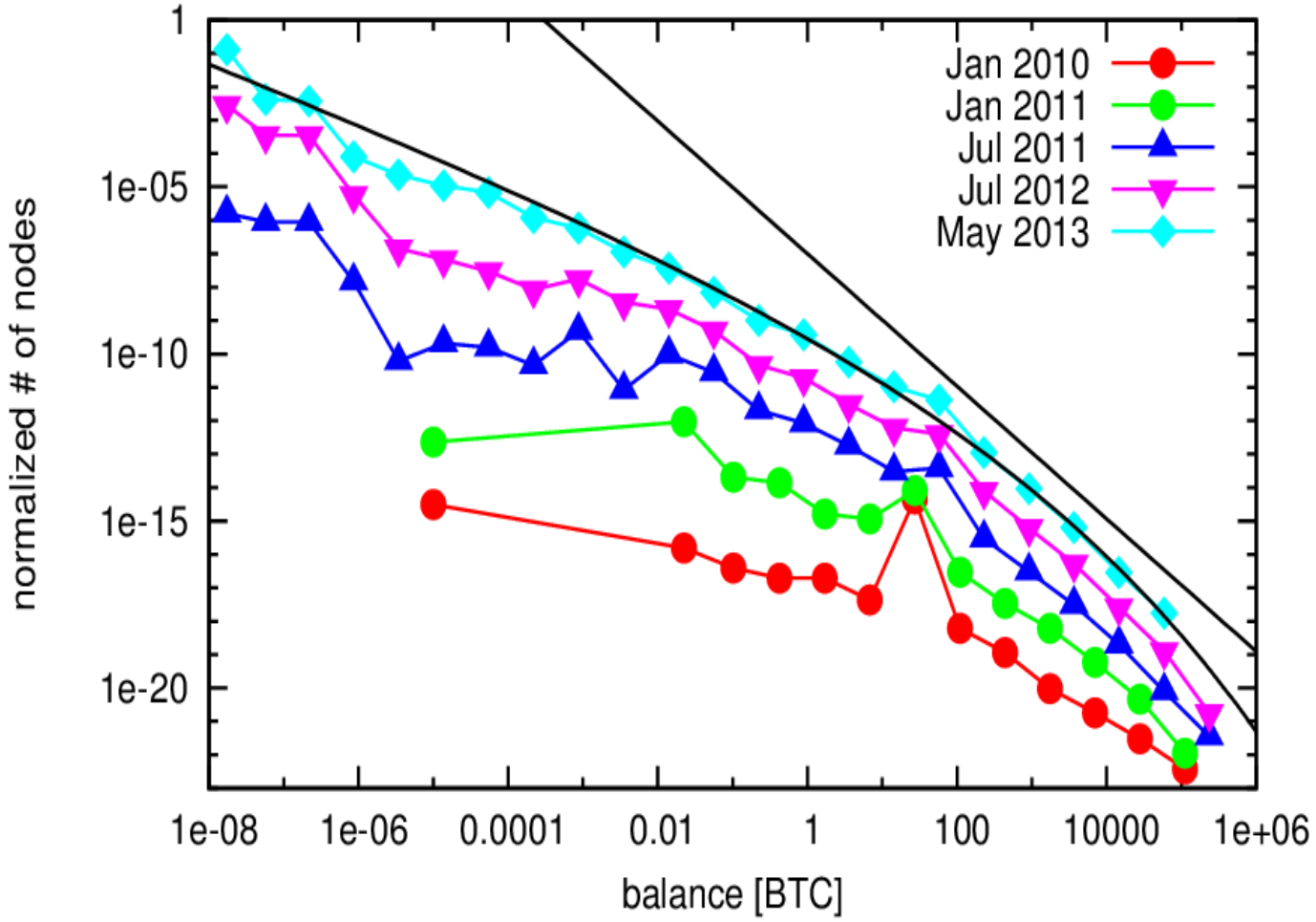


Bitcoin, statisztikák



fokszámeloszlás

Bitcoin, statisztikák



Vagyon eloszlás

Preferential attachment

- Barabási, A., & Albert, R. (1999). Emergence of scaling in random networks. Science, 286, 509–512.
- Barabási, A., Jeong, H., Néda, Z., Ravasz, E., Schbert, A., & Vicsek, T. (2002). Evolution of the social network of scientific collaborations. Physica A, 311, 590–614.
- Newman, M. (2001). Clustering and preferential attachment in growing networks. Physical Review E, 64(2), 025102.
- Wang, X., & Loguinov, D. (2006). Wealth-Based Evolution Model for the Internet AS-Level Topology. Proceedings IEEE INFOCOM 2006.

Preferential attachment

$P(k) \sim k \rightarrow$ fokszámeloszlás $\sim k^{-3}$

“rich-get-richer”

nemlineáris modell: $P(k) \sim k^{\alpha}$

Tesztelés: fokszámok változása adott időtartam alatt

Itt: megvan minden tranzakció, lehet “mikroszkópikus” statisztikákat is használni

Preferential attachment

Teszt: eloszlás visszatranszformálása

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

Megfelelő exponensre az R értékek eloszlása egyenletes lesz

Megvalósítás: minden tranzakcióra R számolása, ez nem triviális

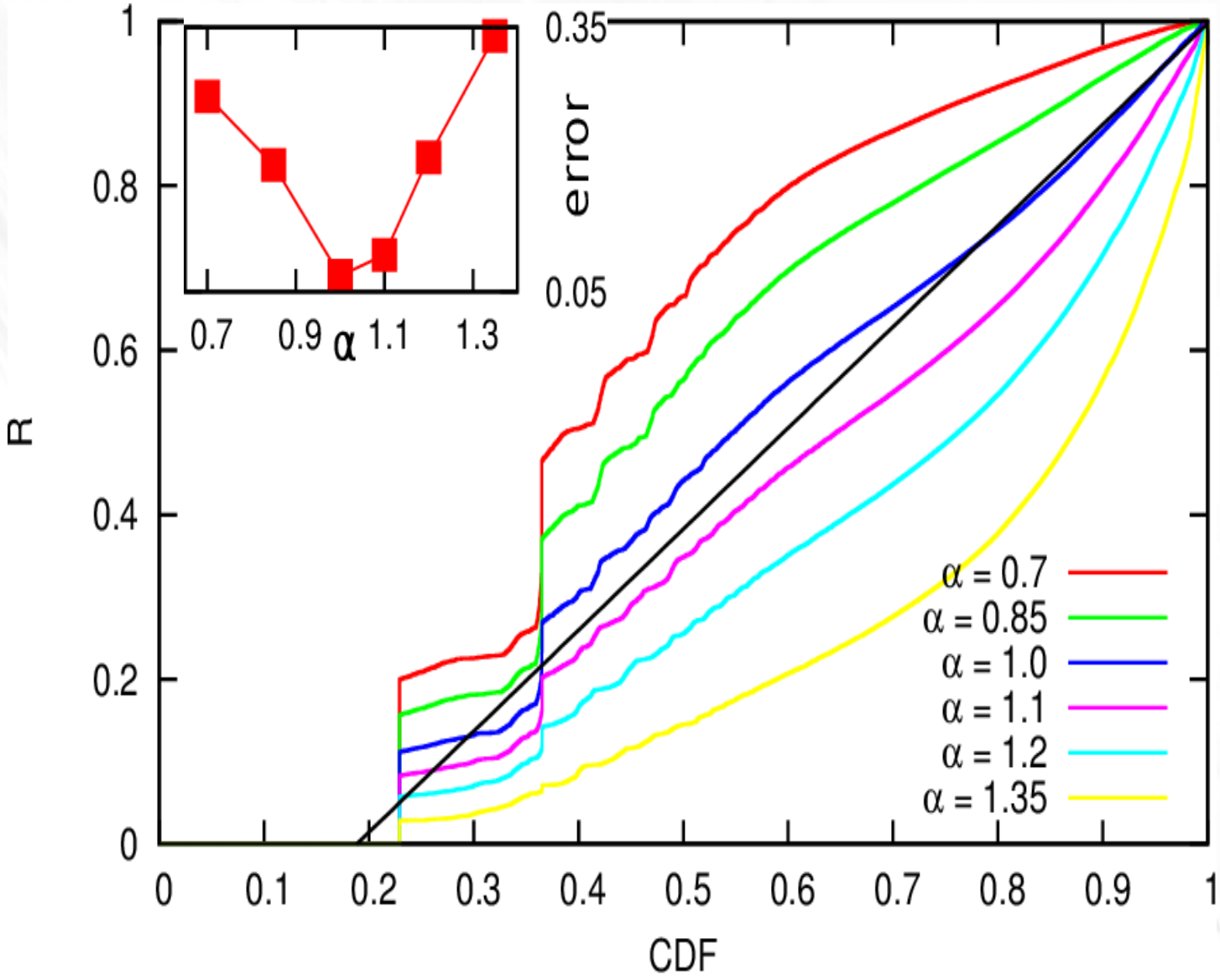
Vagyonokra ugyanígy

Preferential attachment

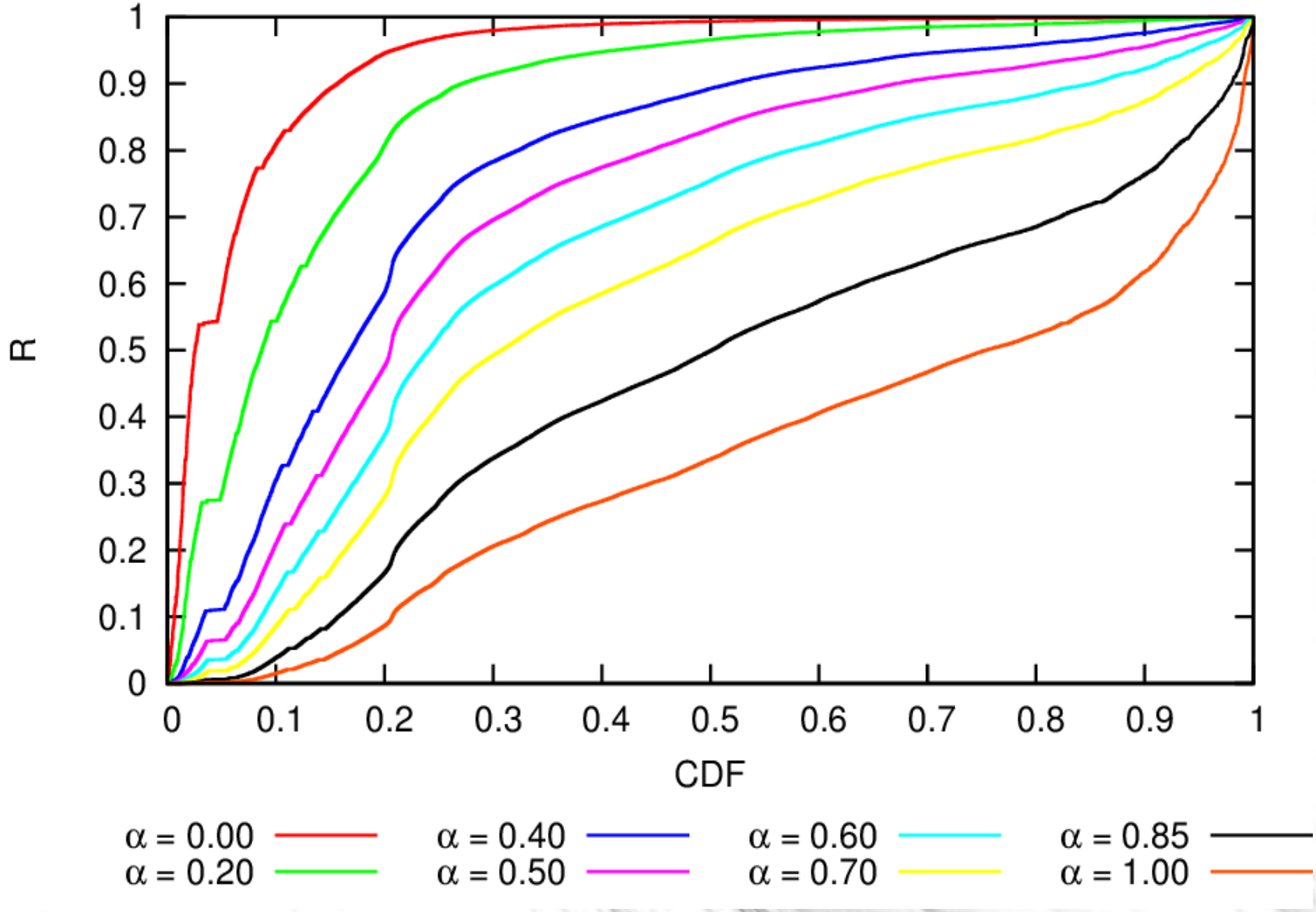
Teszt számolása: adatstruktúrák

- Eloszlás nyilvántartása
- Vagyonoknál: több millió érték megfelelő tárolása
- Hashmap, binary tree, red-black tree, binary heap

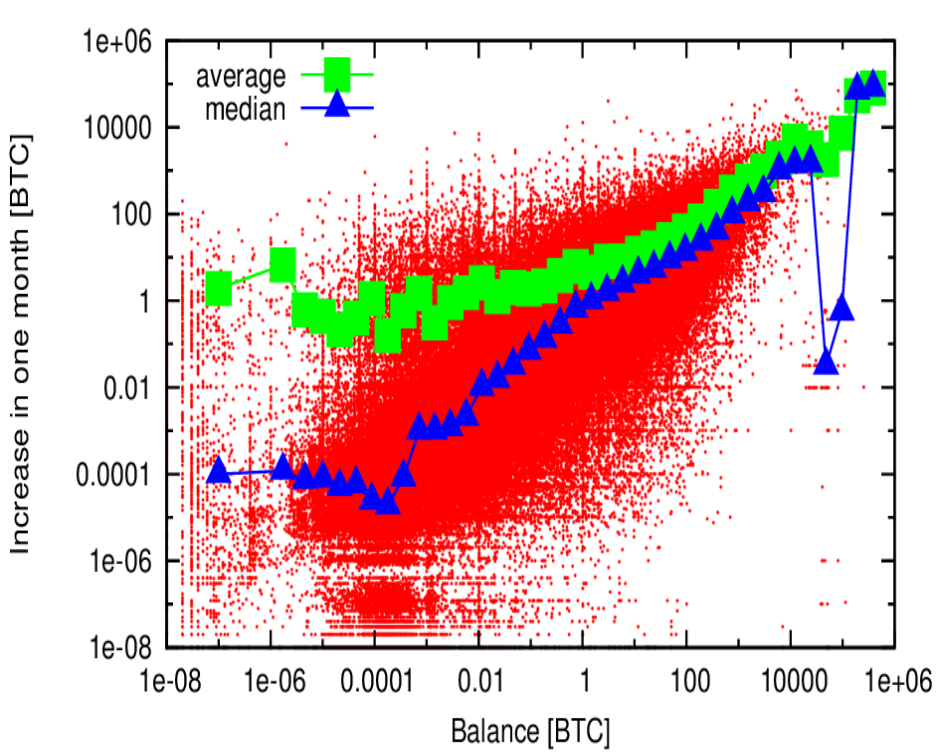
Preferential attachment, fokszámok

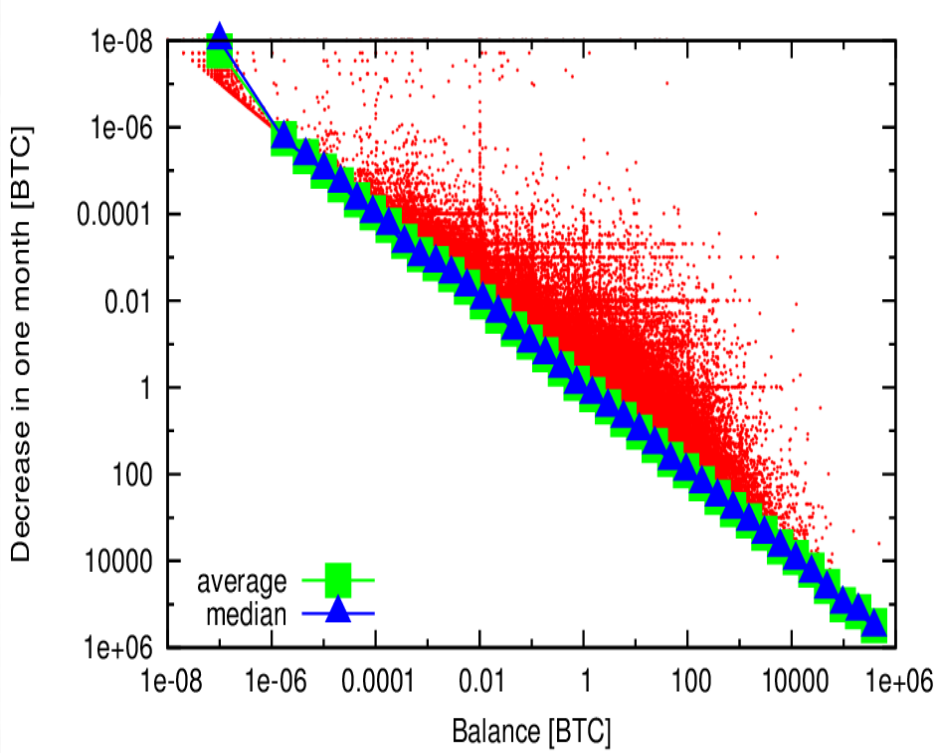


Preferential attachment, vagyonok

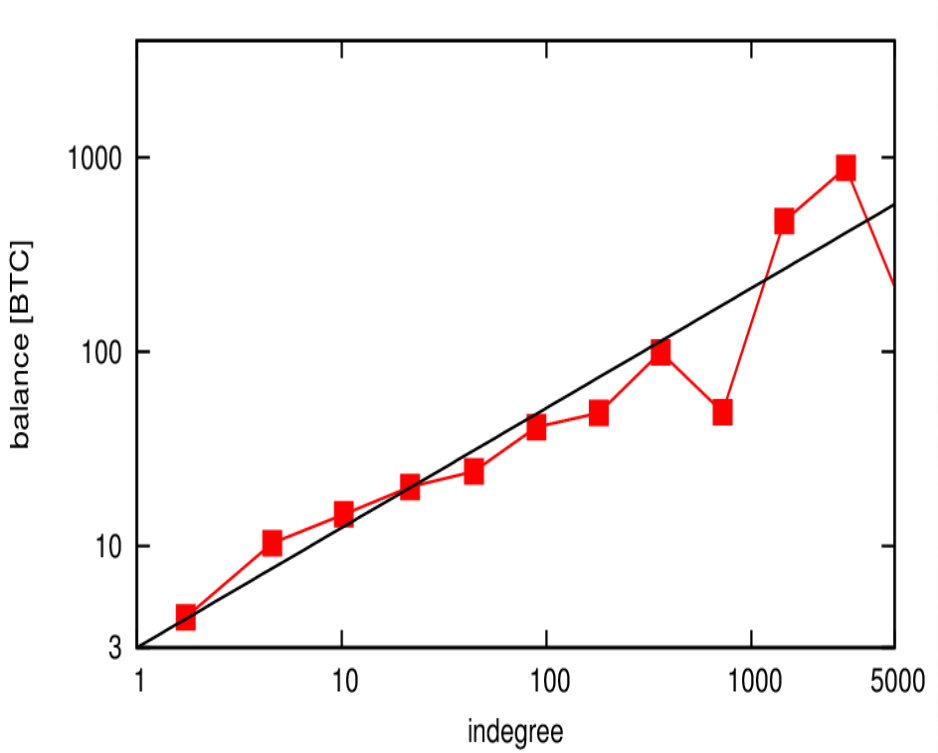


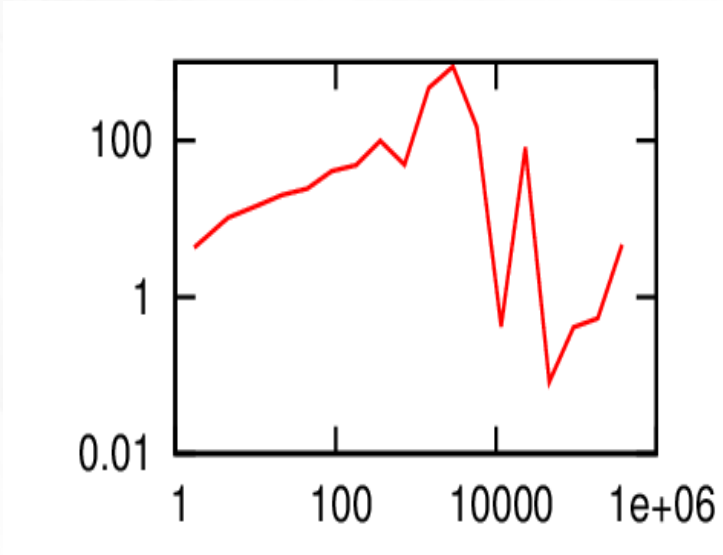
Preferential attachment, vagyonok



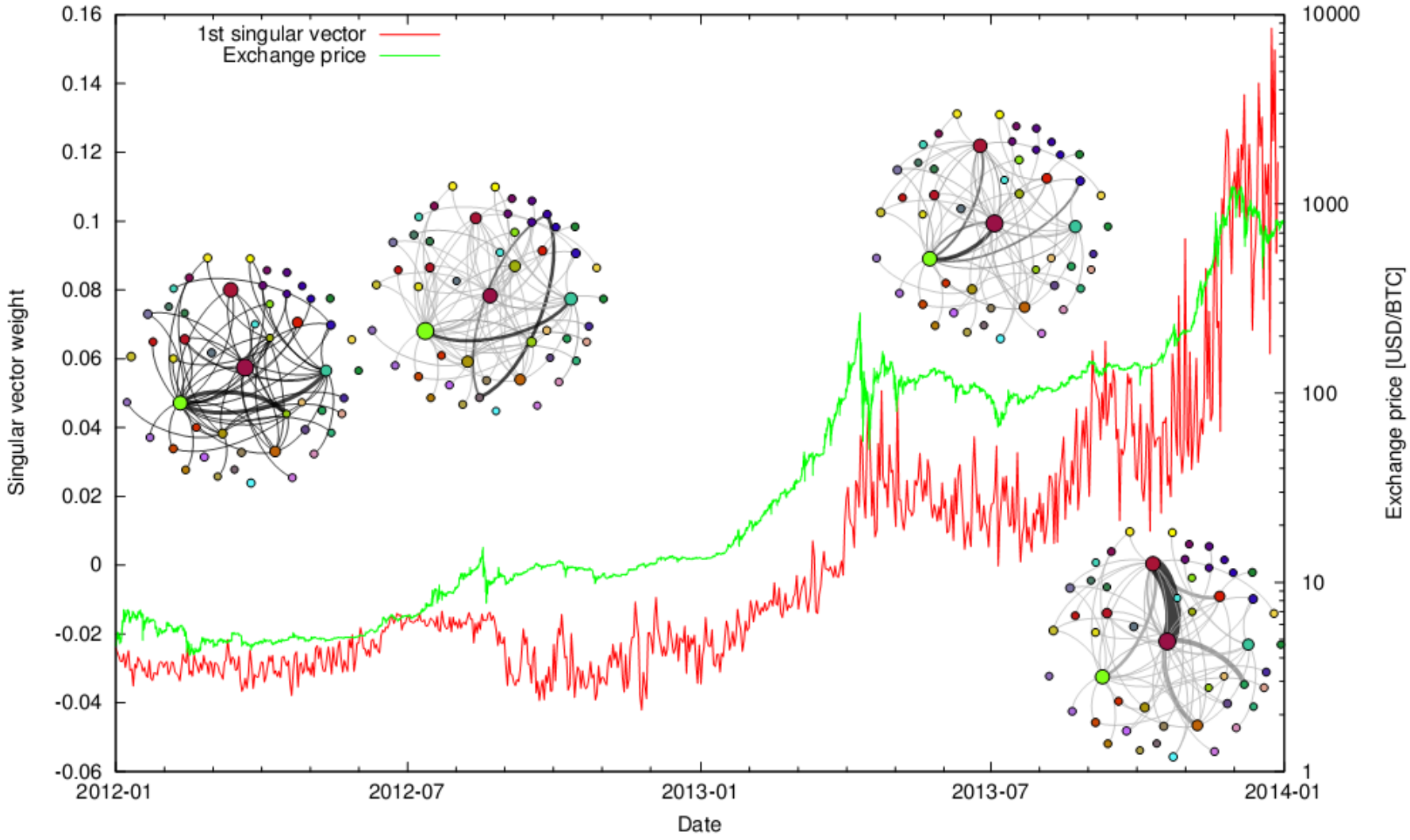


Vagyonok és fokszámok

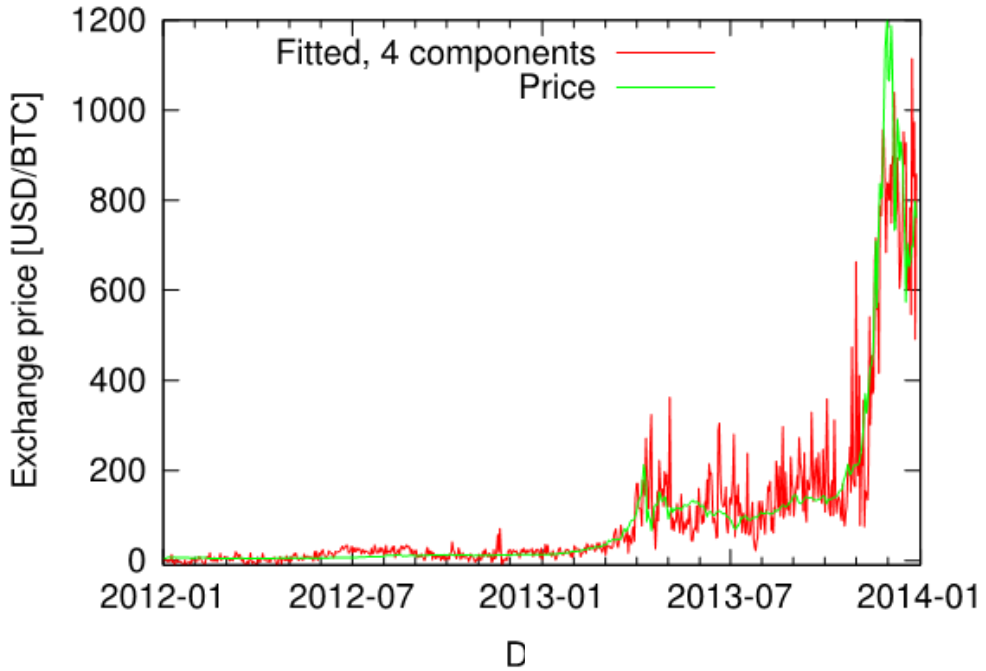


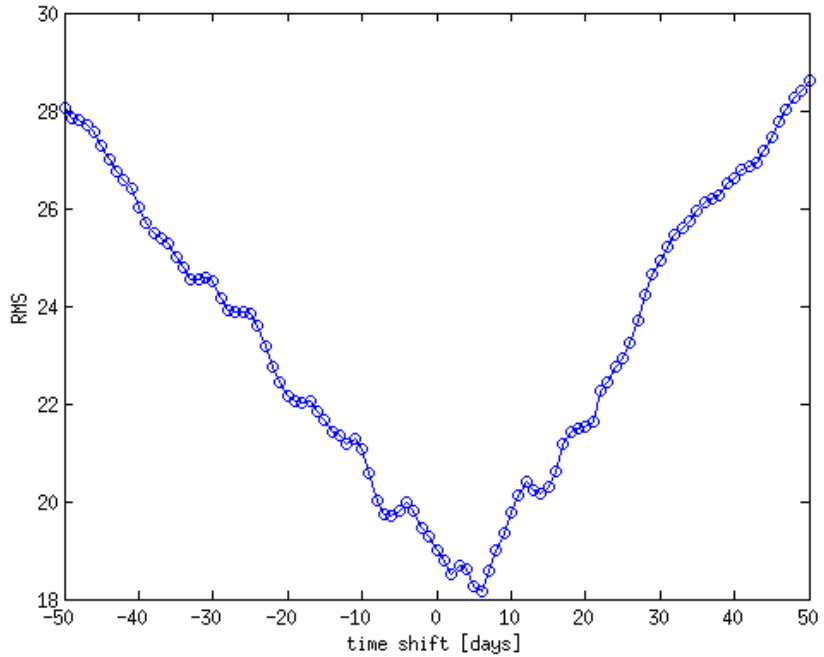


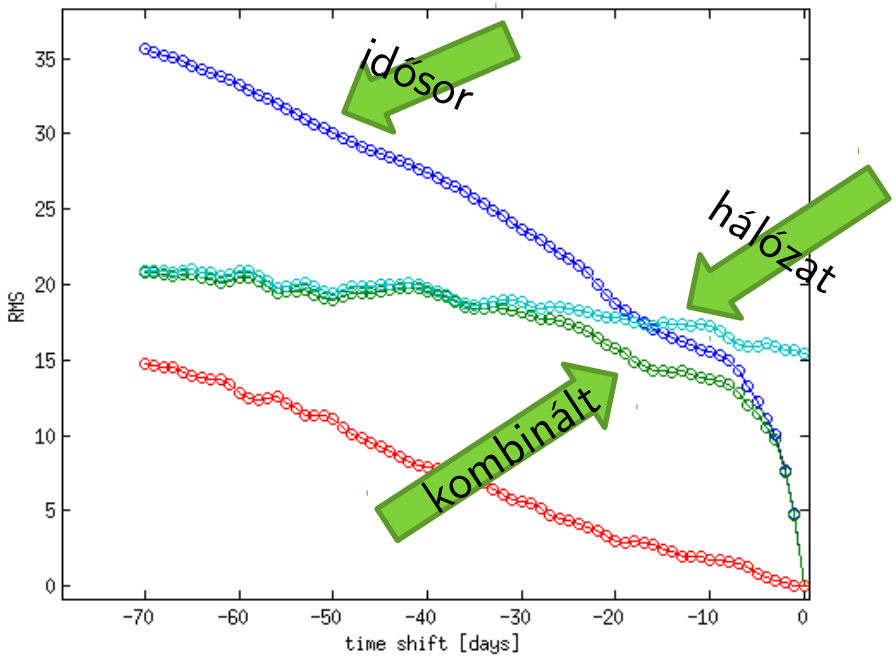
Időbeli változások azonosítása



Időbeli változások azonosítása







Köszönöm a figyelmet!

Do the rich get richer? An empirical analysis of the BitCoin transaction network; D Kondor, M Pósfai, I Csabai, G Vattay; PloS one 9 (2), e86197 (2014)

Inferring the interplay of network structure and market effects in Bitcoin; D Kondor, I Csabai, J Szüle, M Pósfai, G Vattay; New Journal of Physics, New J. Phys. 16 125003. (2014)

www.vo.elte.hu/bitcoin

kondor.dani@gmail.com