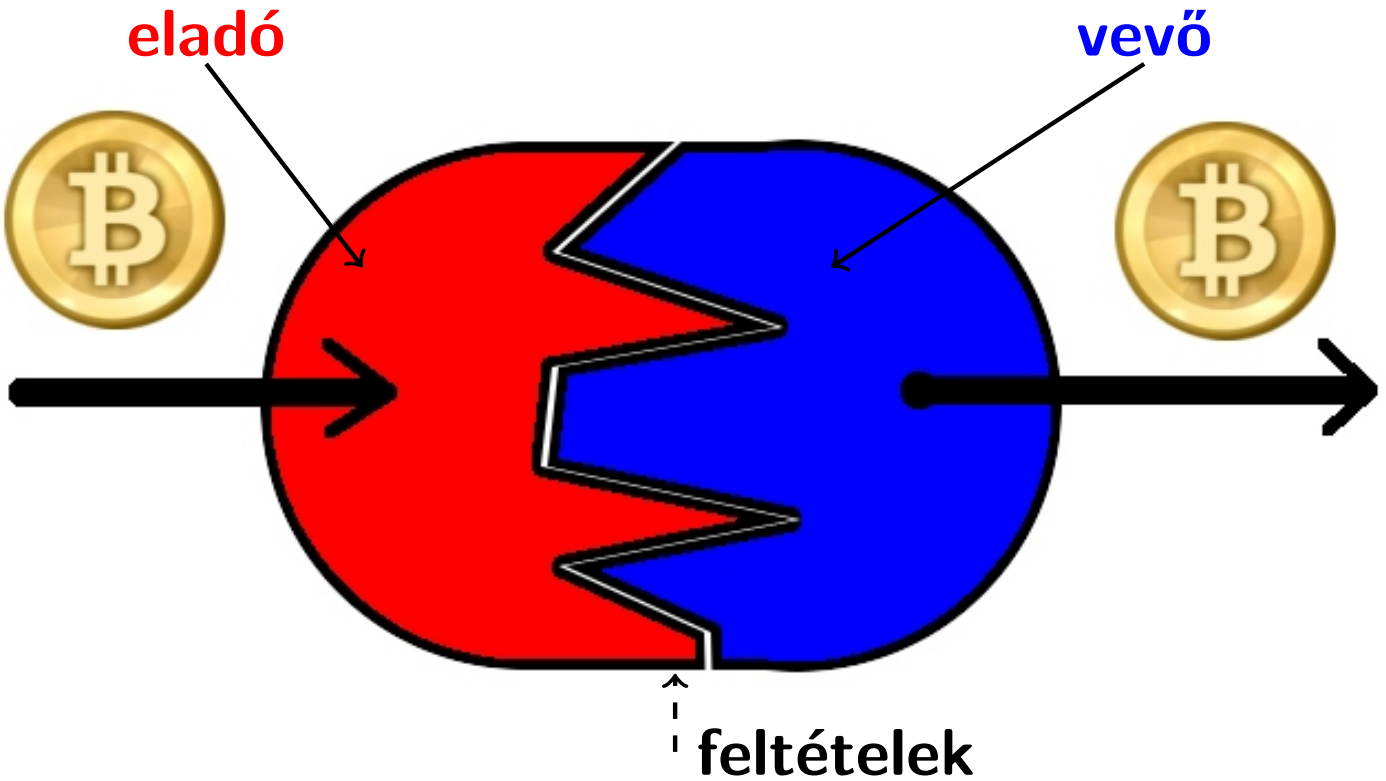

BITCOIN


és ami mögötte van...
21 BTC
(total)
Bob
wallet
private
ys (A,C,D)
Bob's wallet
has 2 private
keys (B,E)
Csirmaz László, CEU
Networkshop, 2014, Pécs

Tartalom

Én eladok, te veszel

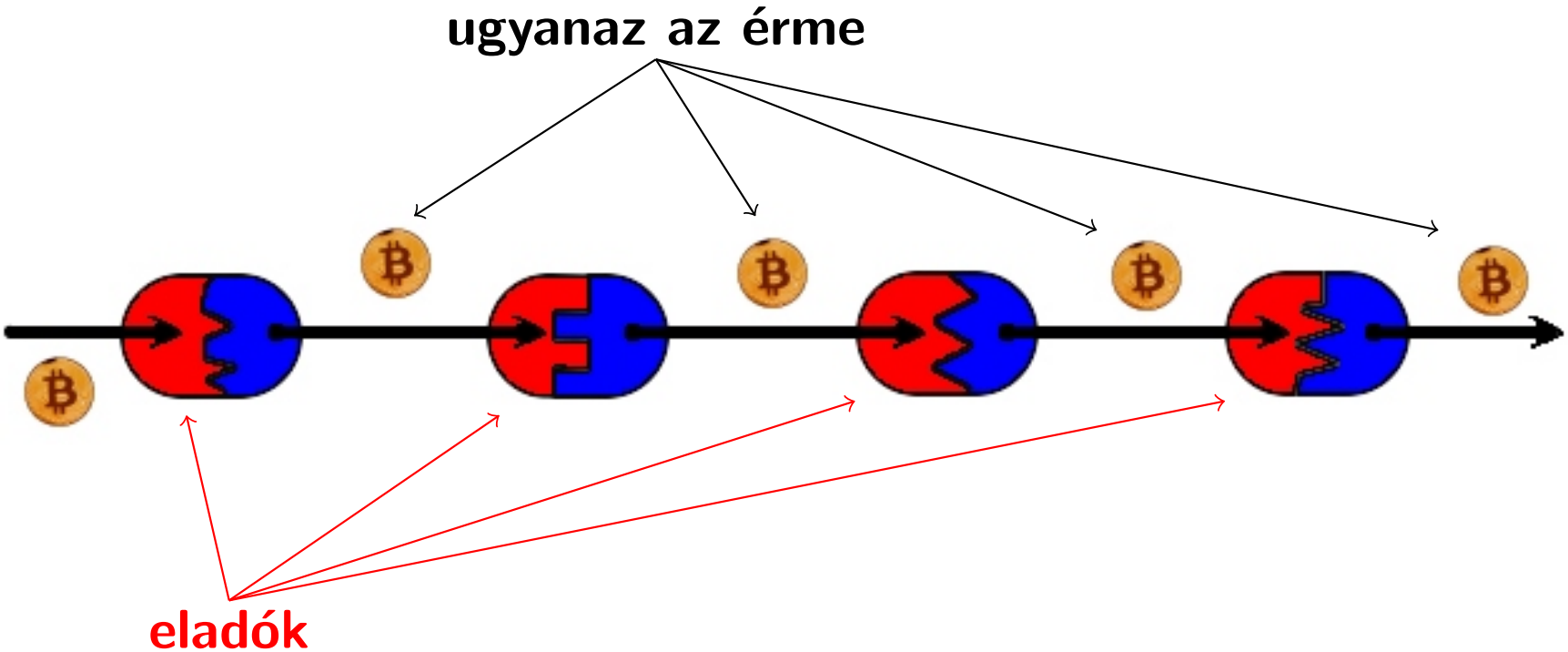


Tipikus **feltételek**:

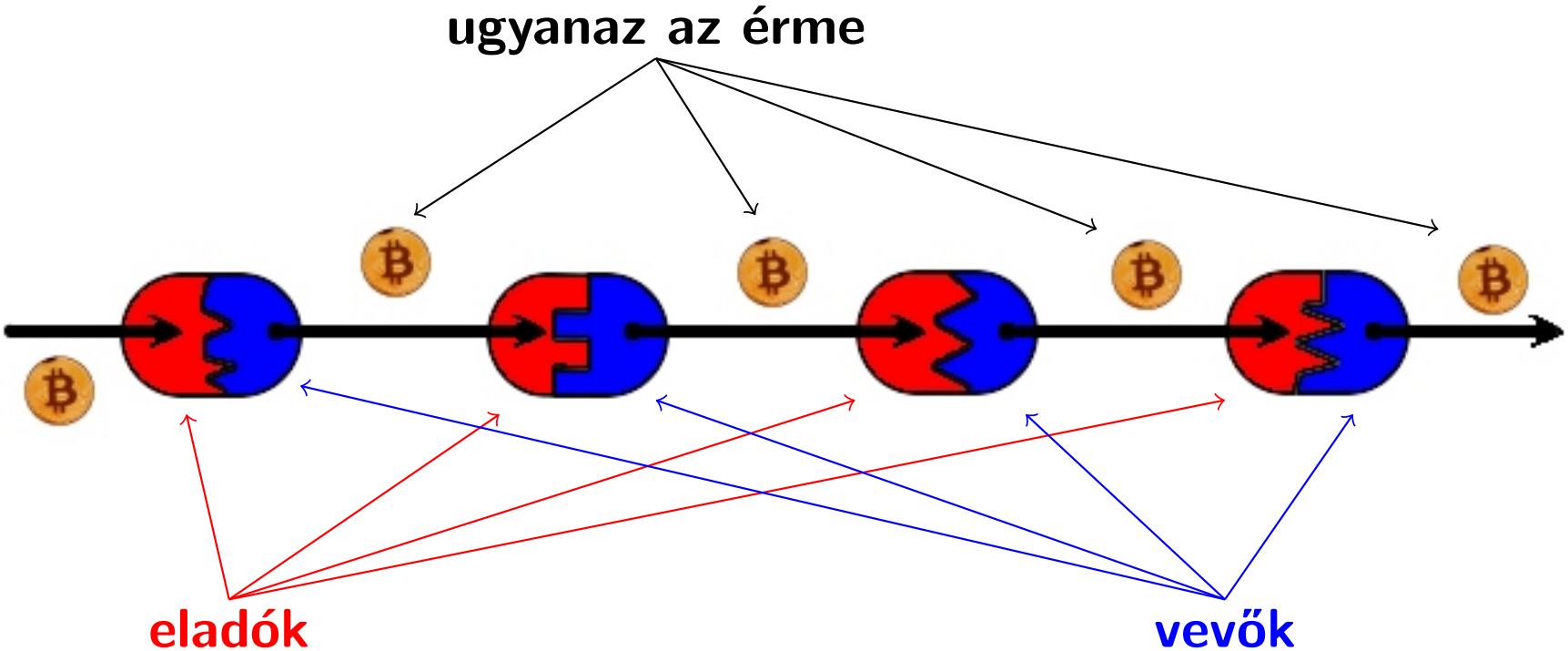
Itt van **egy** nyílvános kulcs, írj alá valamit. Itt van!

Itt van **három** nyílvános kulcs, legalább 2-vel írj alá. Itt van!

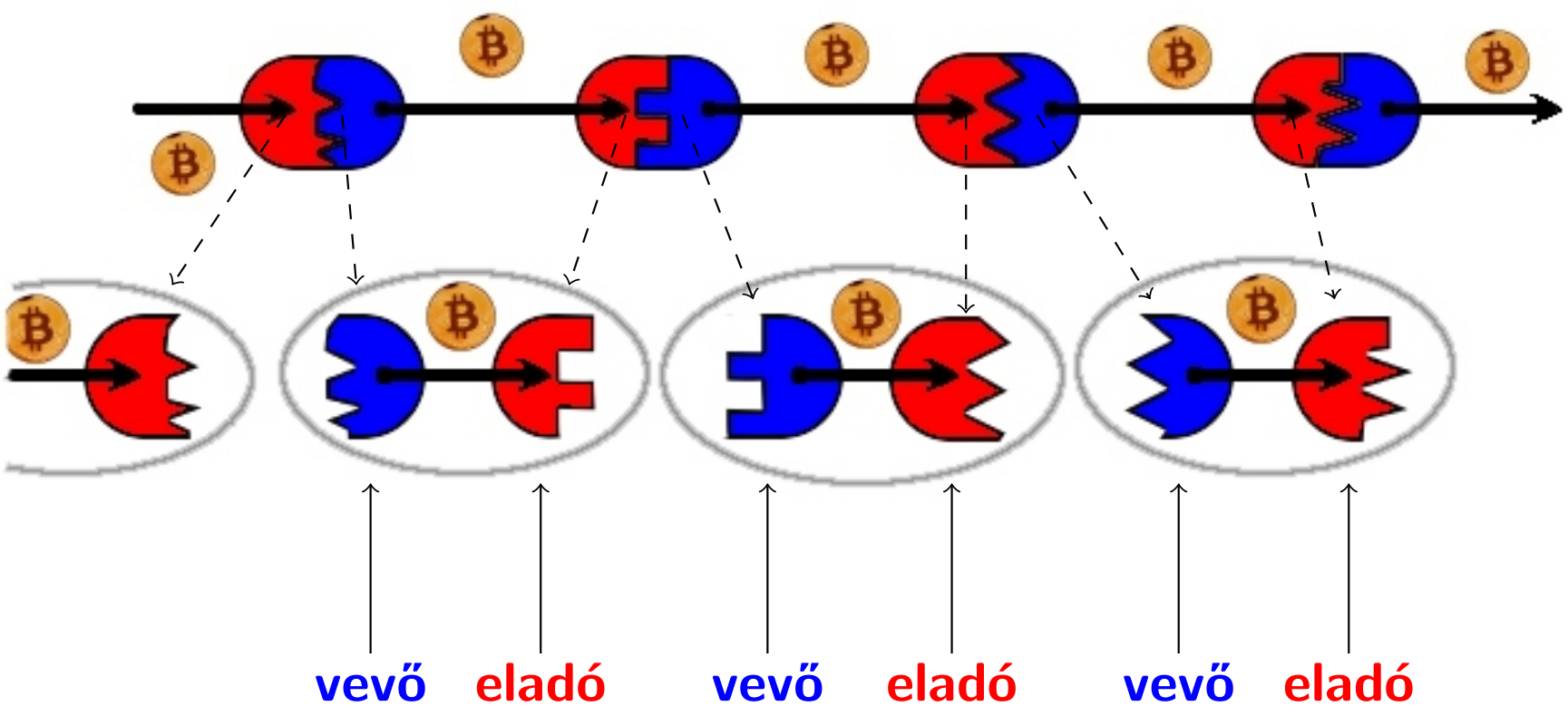
A pénz(érme) útja



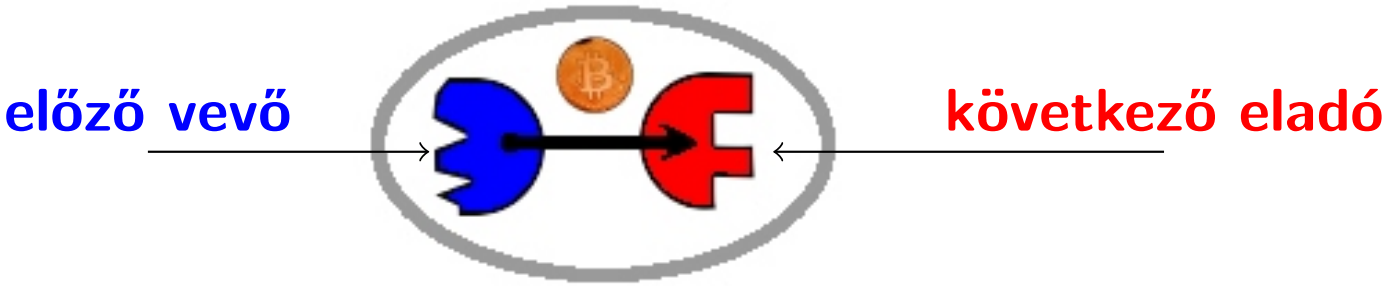
A pénz(érme) útja



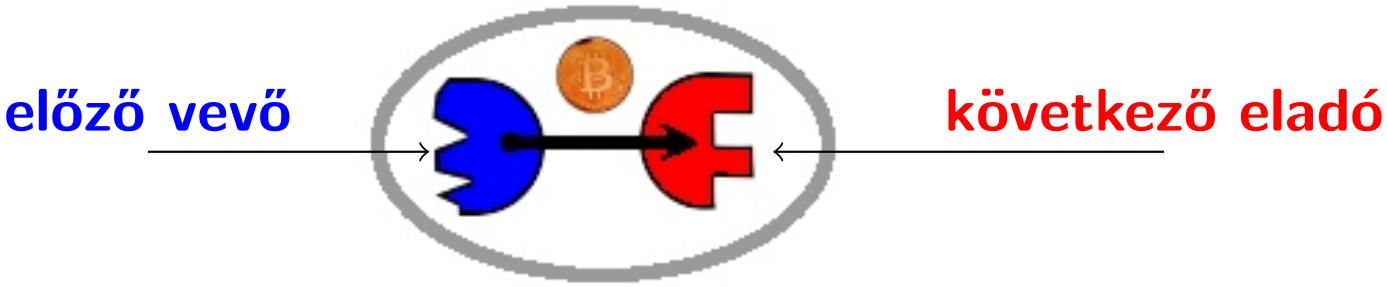
Hogy látja ezt a bitcoin?



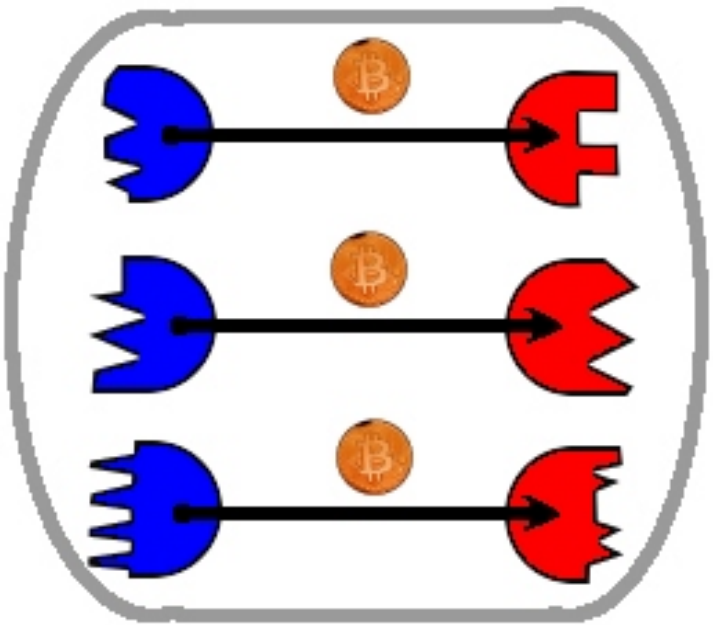
Egy bitcoin tranzakció



Egy bitcoin tranzakció

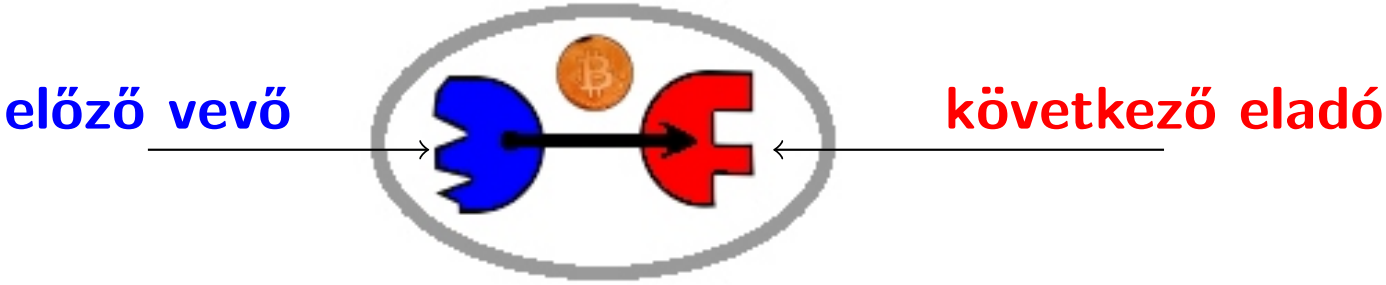


vagy inkább (gazdaságosabb):

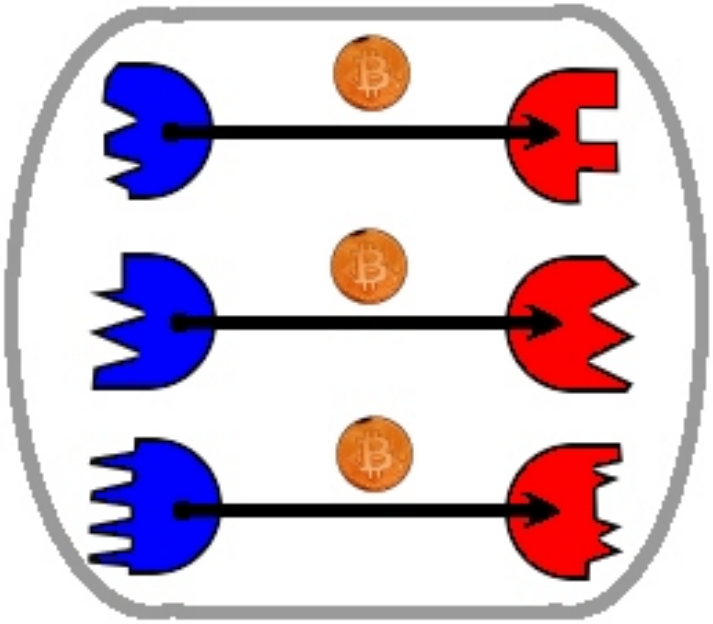


Az érméket nem lehet bontani!

Egy bitcoin tranzakció



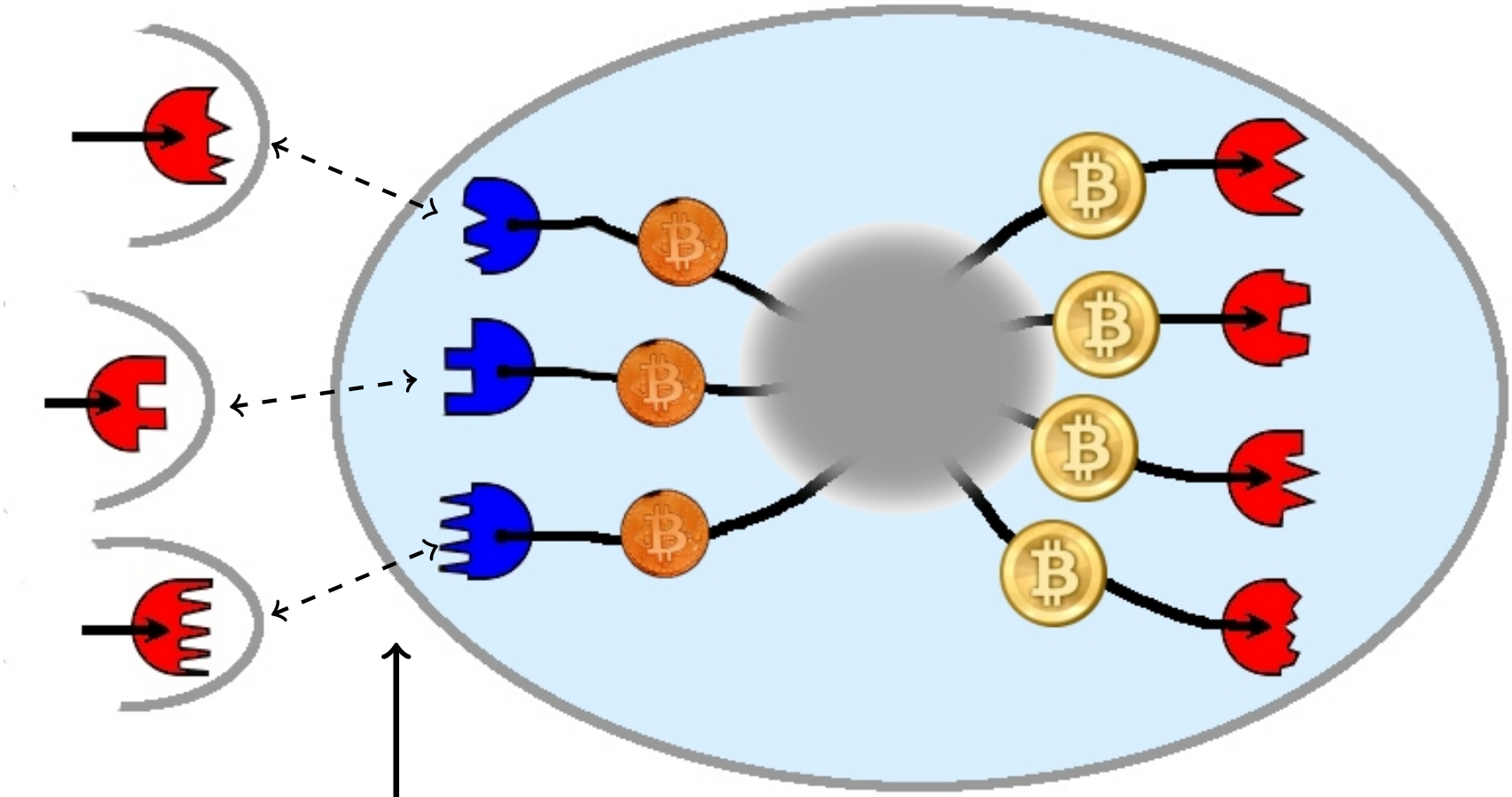
vagy inkább (gazdaságosabb):



Az érméket nem lehet bontani!

Hogyan kapjuk meg
a visszajáró aprót?

Sztenderd bitcoin tranzakció

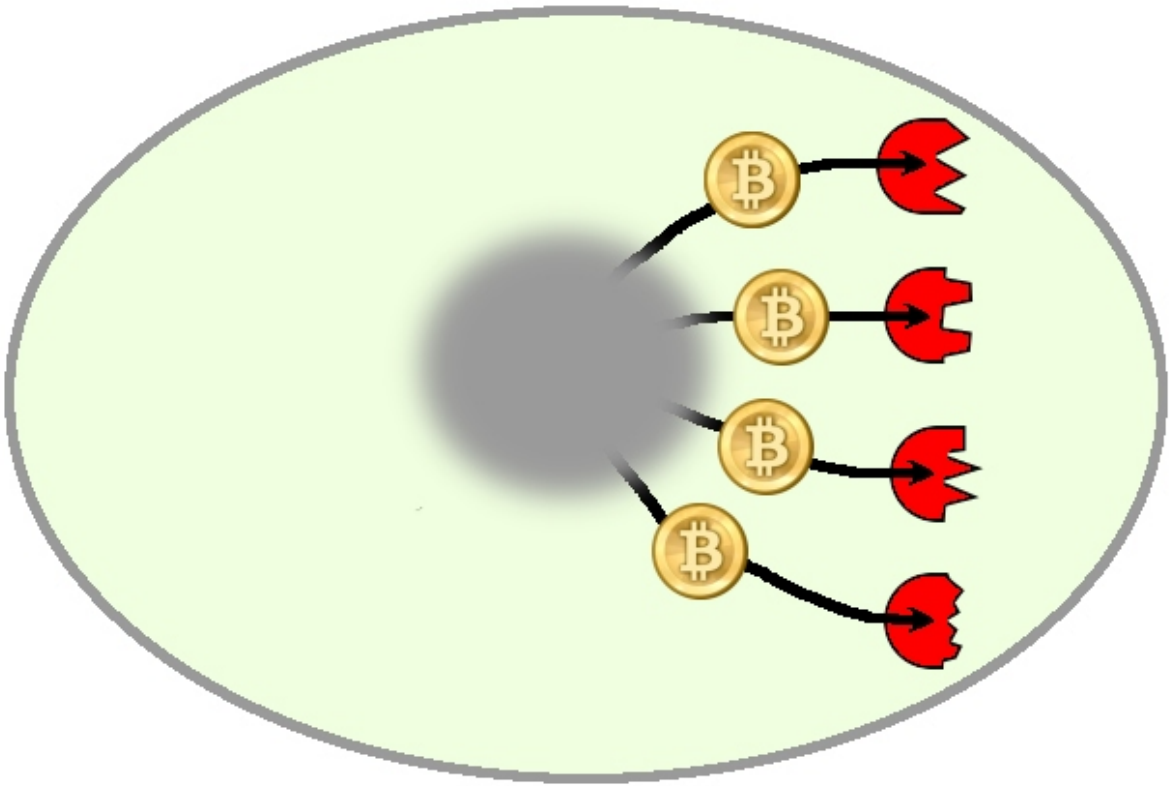


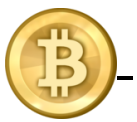
Mindnek kell párja legyen korábbról

A kimenő összeg nem lehet több, mint ami bejött

Coin-base tranzakció

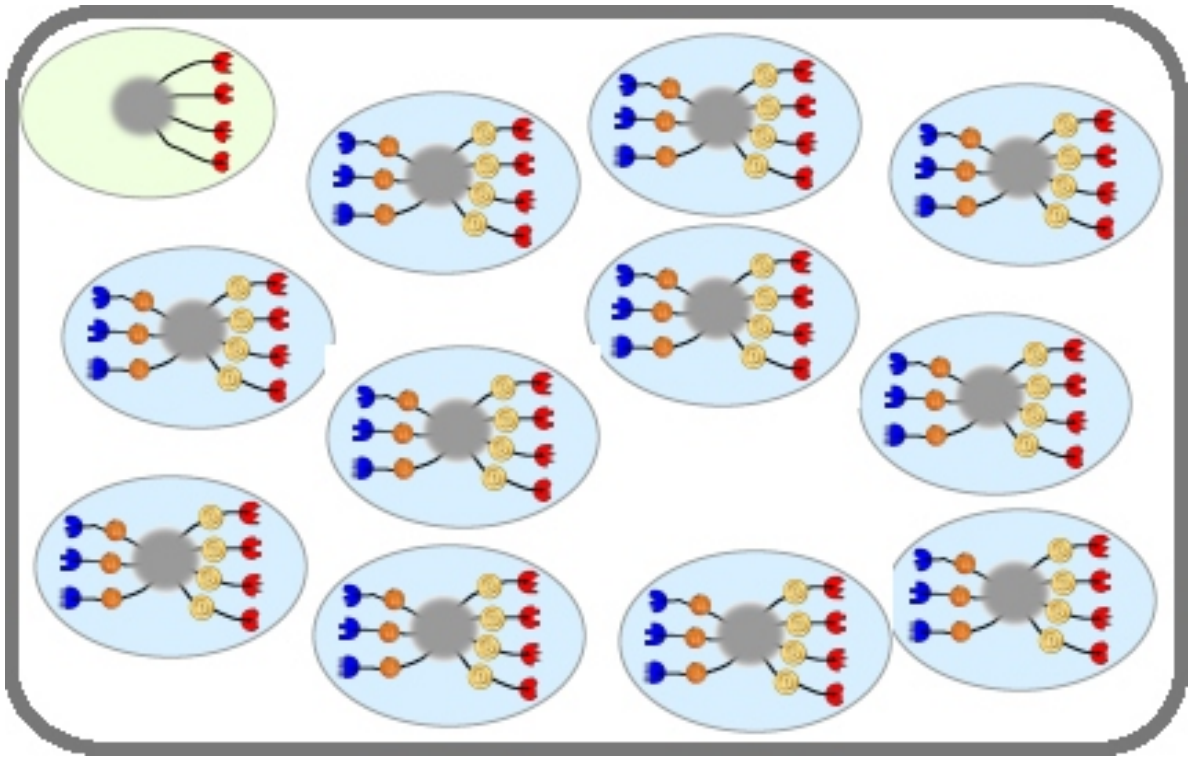
Hogyan keletkeznek az érmék?



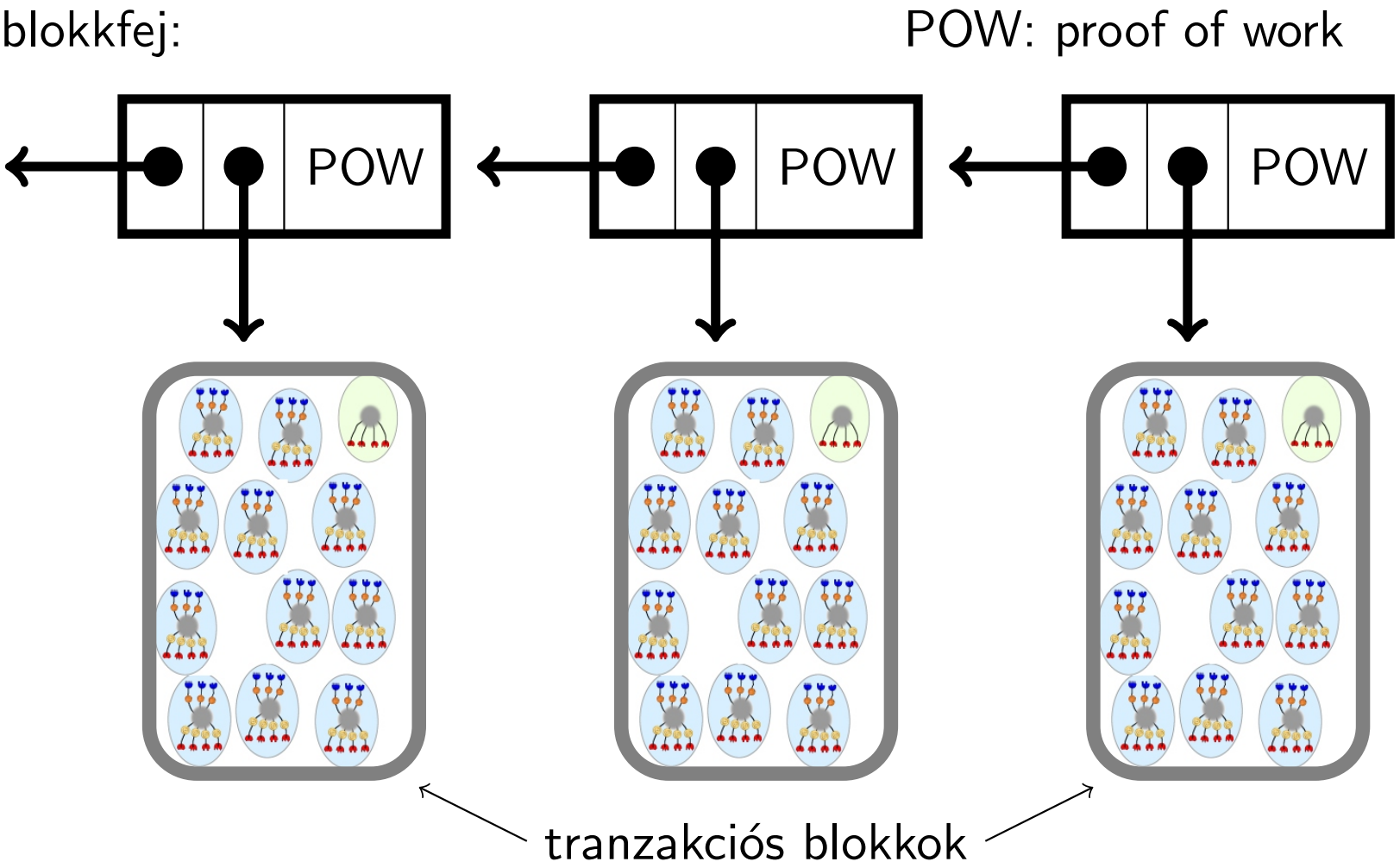
Minden  -t egy ilyen **coin-base tranzakció** hoz létre.

Tranzakciós blokk

Pontosan egy *coin-base* tranzakció, és sok-sok *sztenderd* tranzakció egy blokkban:



Bitcoin blokklánc



Minden 10 percben egy új blokk készül.

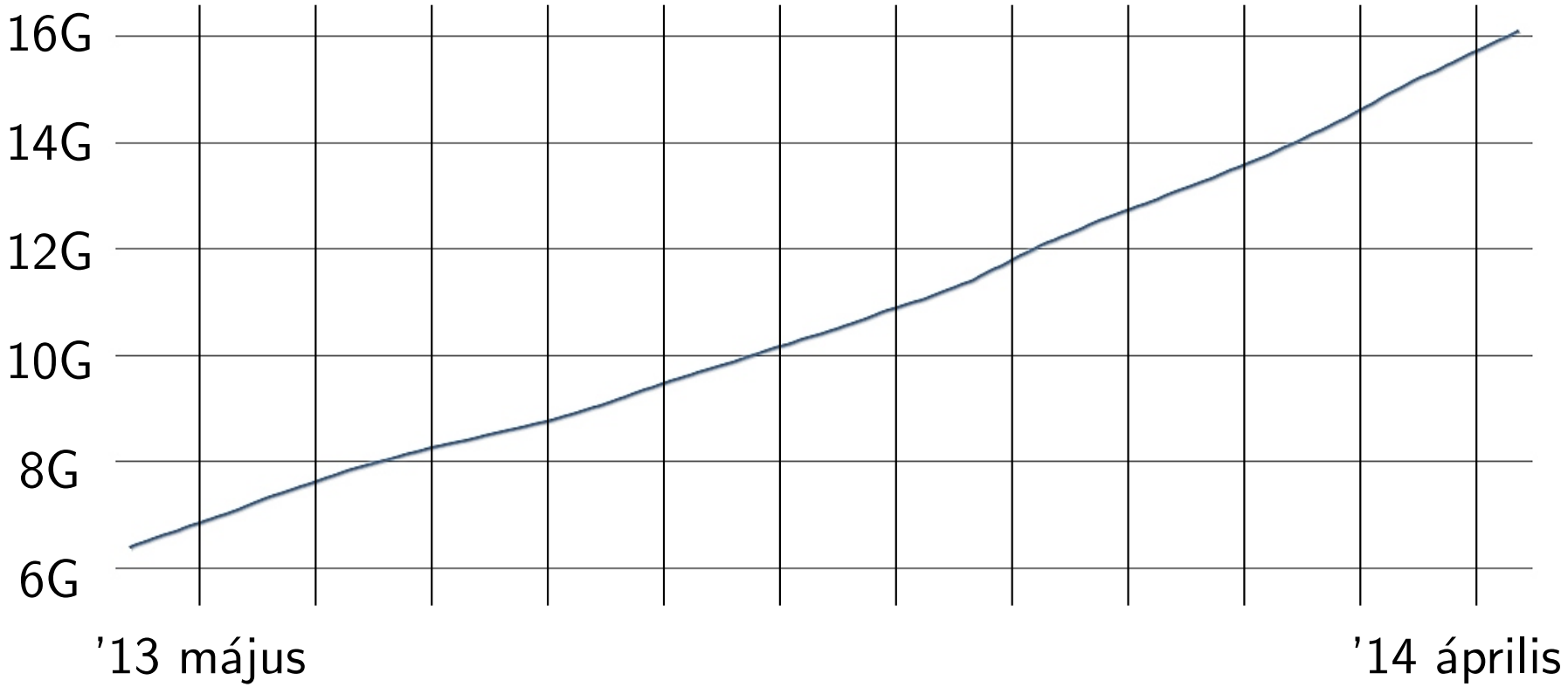
A blokklánc

A bitcoin igazi újítása

- Nyilvános
- P2P hálózat (mint bittorrent, skype, streaming), nincs központ
- A **bányászok** tartják karban – konszenzus
- Lekérdezhető: `http://blockchain.info` (szolgáltatás)
- A korai kliensek saját példányt tartottak ($>$ 1 nap a letöltés)
- Jelenleg 16G; a mérete a tranzakciók számával arányosan nő; tavaly +8G
- **Minden** tranzakció nyilvános és vizsgálható, visszakereshető
- Sok minden másra is jó – **vigyázat, utánozzák!**

A blokklánc mérete

Blokkok ≈300,000, tranzakciók ≈36.5 millió (2014 áprilisig)
Az adatméret változása egy év alatt:

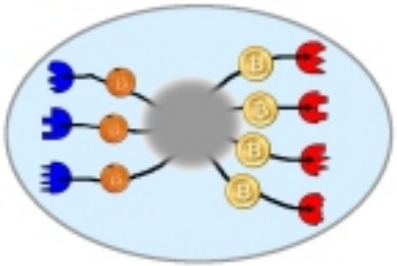


Forrás: blockchain.info

Tartalom

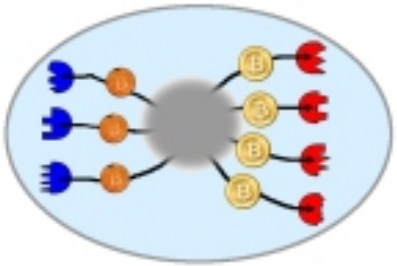
Hogyan használjuk?

- Összeállítunk egy tranzakciós blokkot:



Hogyan használjuk?

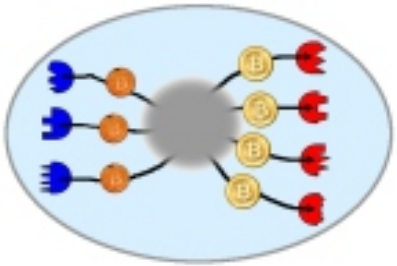
- Összeállítunk egy tranzakciós blokkot:



- Bedobjuk (feltöltjük) a “pool”-ba:

Hogyan használjuk?

- Összeállítunk egy tranzakciós blokkot:

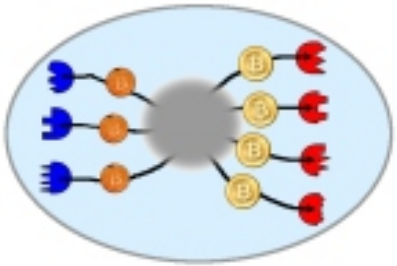


- Bedobjuk (feltöltjük) a “pool”-ba:

- Megvárjuk, míg a tranzakciónk megjelenik a blokkláncban:

Hogyan használjuk?

- Összeállítunk egy tranzakciós blokkot:



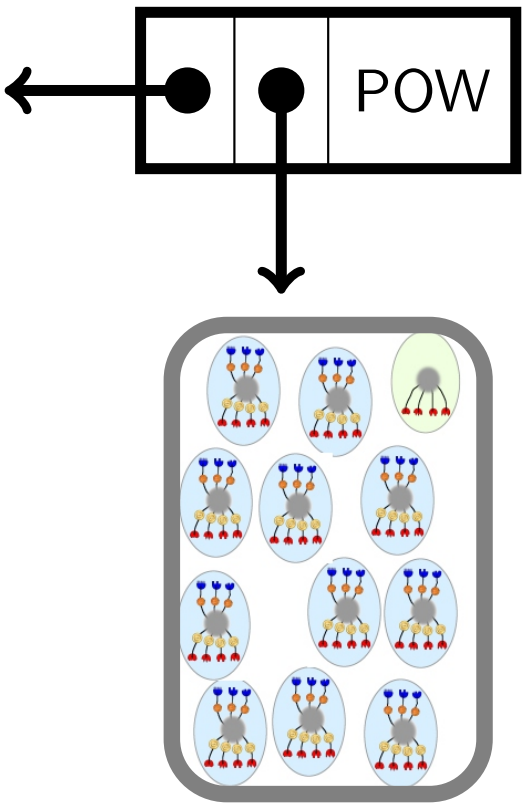
- Bedobjuk (feltöltjük) a “pool”-ba:

- Megvárjuk, míg a tranzakciónk megjelenik a blokkláncban:

- Örülünk:

Tartalom

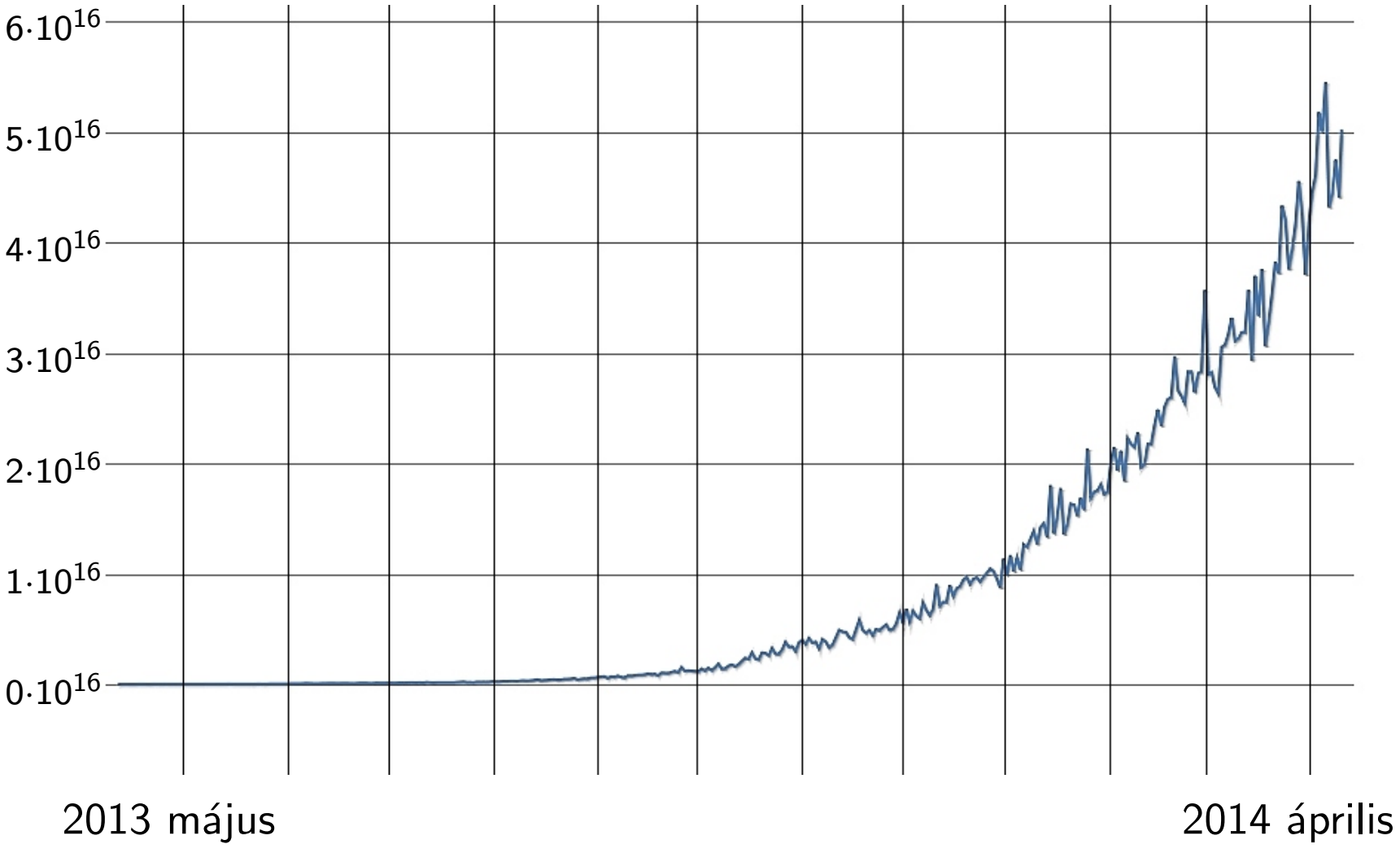
Bicoin bányászat – egy új blokk előállítása



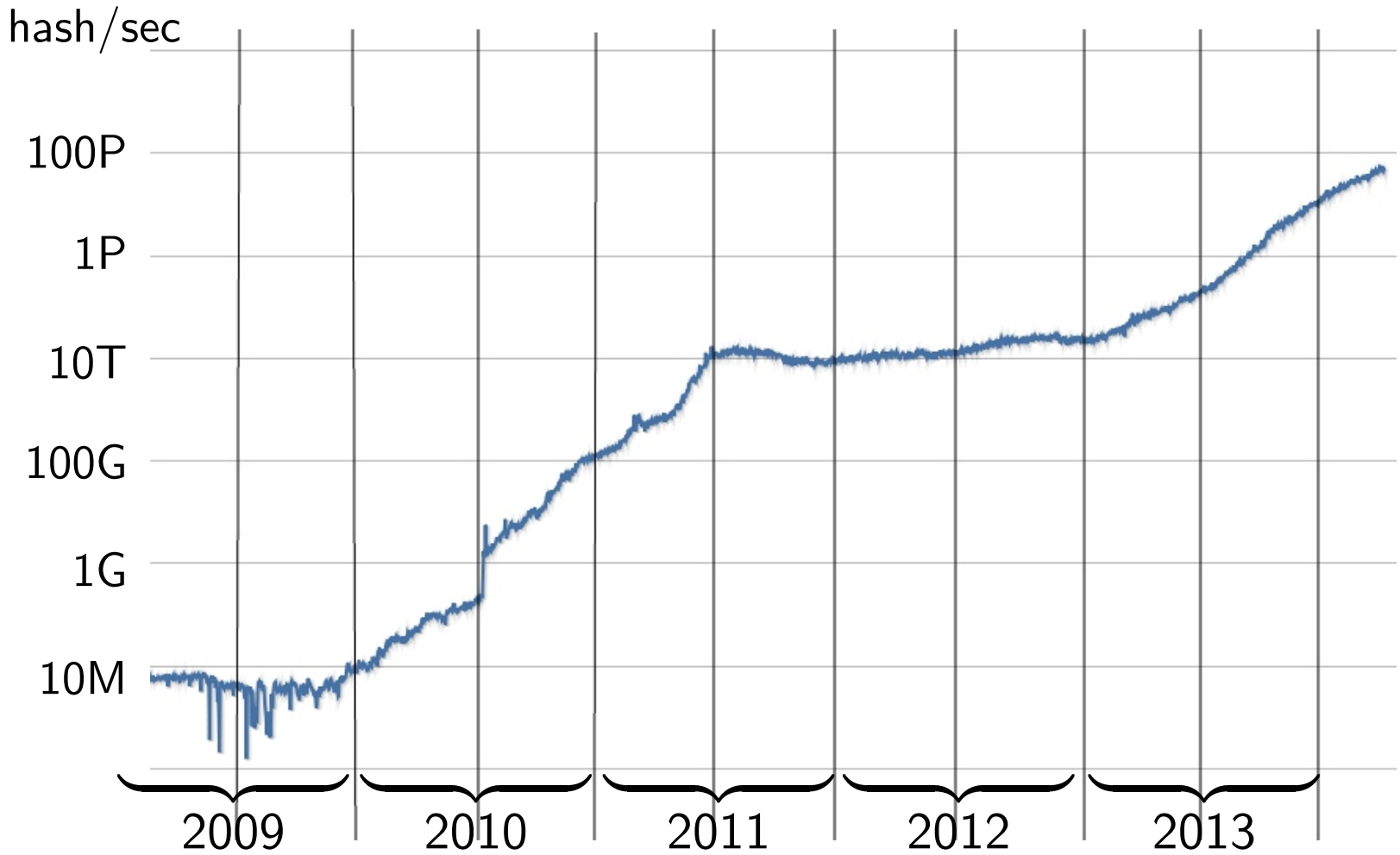
A bányász állítja össze a tranzakciós blokkot "pool"-ból, és adja hozzá a coin-base tranzakciót saját hatáskörében, ami ma
25 bitcoin plusz a nem elköltött pénz
(ez a fix rész minden 2 évben feleződik)

POW – egy véletlen szám, amivel együtt a blockfej hash-e sok-sok nullával kezdődik (a "sok" most 64)
A nullák száma előírt és kéthetente változik
Átlagban minden 10 percben áll elő egy új blokk
64 nulla bithez átlagosan 2^{64} hash-t kell kiszámítani

Mennyit kell dolgozni a POW-hoz? (hash/sec)



POW változása a kezdetektől logaritmikus skálán

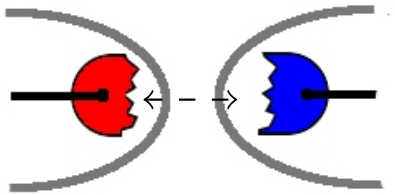


Forrás: blockhain.info

Tartalom

Kripto használat

Viszonylag kevés – az igazi ötletekhez nem kell!

1. Az összeillő tranzakcióknál: 
   - “itt van egy nyilvános kulcs”
   - “tudom a hozzá tartozó titkos kulcsot” (proof of knowledge)
2. A “pool”-ba feltöltött tranzakciók integritása és szilárdsága:
   - ne lehessen a tranzakciót átírni, részleteit megváltoztatni (más címzett, más összeg, stb);
   - több tranzakcióból újat összetenni;
   - érvényes tranzakciót érvénytelenné tenni (dupla költés)

Kripto használat – konklúzió

– Mindkét fenti kérdést **hiba nélkül** oldja meg.
– A bitcoin fennállása óta (2009) nem volt sikeres kripto támadás.

De . . .

Kripto használat – konklúzió

– Mindkét fenti kérdést **hiba nélkül** oldja meg.
– A bitcoin fennállása óta (2009) nem volt sikeres kripto támadás.

De . . .

1. A két feladat nincs szétválasztva, noha független megoldás kellene.
2. Az integritás a felhasználóra van bízva, zavaros és nehezen áttekinthető, nincs világos cél és arra irányuló megoldás. A "kincstári" (default) tranzakciók viszont biztonságosak.
3. A rosszindulató felhasználó át tudja írni érvényes tranzakcióját – *malleability bug* –, ezzel úgy tehet, mintha a tranzakció nem került volna végrehajtásra. Ez nem **hiba**, de semmiképpen nem elegáns.

Tartalom

Nagyobb bitcoin lopások

Nem az alap protokollt támadták, hanem a szolgáltatásokat.

Dátum	Hely	Típus	eltünt BTC	USD érték
2011 jún	Mt.Gox	exch	2,000	$47,000
2011 jún	MyBitcoin	wallet	79,000	$1,100,000
2012 május	Bitconica	exh	38,000	$91,000
2012 jún	Bitconica	exch	40,000	$305,000
2012 szept	Bitfloor	exch	24,000	$250,000
2013 okt	Inputs.io	wallet	4,100	$1,200,000
2013 nov	GBL (Kína)	exch	4,100	$4,100,000
2014 feb	Mt.Gox	exch	850,000	$500,000,000
2014 már	Flexcoin	wallet	900	$600,000

Pénz-e a bitcoin?

A **pénz** funkciója, szerepe szerteágazó és bonyolult, közgazdasági definíciója sokrétű. A pénz

- értékmérő
- értékálló (megtakarítás!)
- általános csereeszköz
- a csereeszközként azonnali és feltétlen, nem vitatható
- csereszabatos (egyik érme ugyanolyan mint a másik)
- követhetetlen (privát), stb, stb.

Ezek közül a bitcoin többet nem teljesít mint igen (vagy mint más korábbi elektronikus pénzek).
Az amerikai, holland, kínai, ausztrál, orosz . . . törvények szerint

a bitcoin NEM pénz!

A bitcoin sikerének titka

1. Kitünő pénzátutalási módszer: gyors, olcsó(!), megbízható
   Vendégmunkások használják a fizetésük hazautalására (drága banki szolgáltatás helyett)

2. Inkább társadalmi jelenség:
   Miért lett a facebook/twitter/flickr/youtube a vezető, és nem a többi száz ilyen szolgáltatás?

Köszönöm a figyelmet!