Elosztott működésű adatbázisok kihívásai

Erős Levente, 2018-2023.

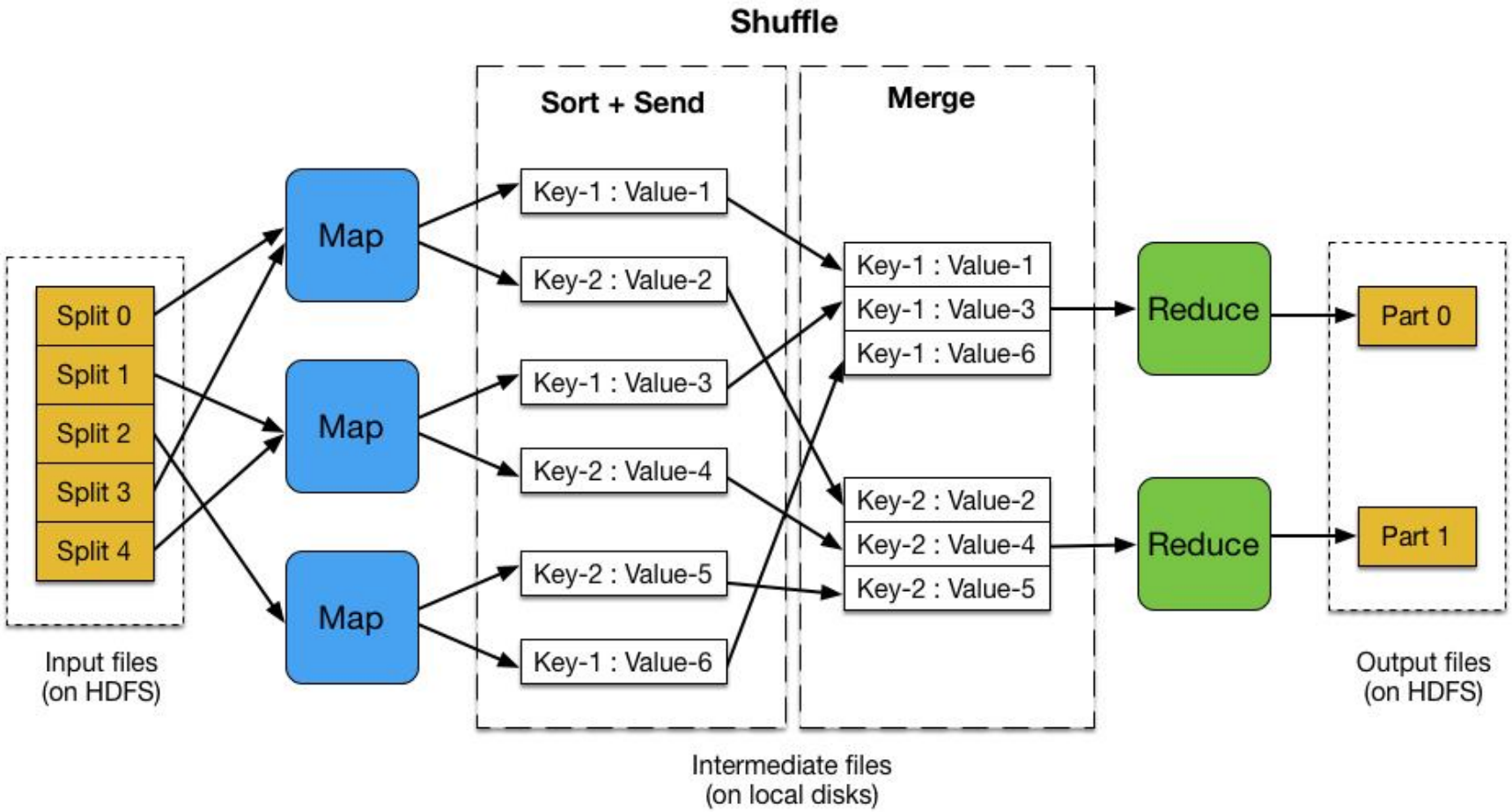
Alapprobléma

- Növekvő
  - Adatmennyiség
  - Felhasználószám
  - Biztonsági igények
- Mi a válasz ezekre?
  - Ezek(egy részé)re partikuláris megoldások
- Két módszert mutatunk be – két cél
  - Map-Reduce
    - módszertan adott típusú lekérdezések párhuzamos, hatékony megoldására
  - Blockchain és Bitcoin
    - decentralizált, teljesen elosztott, kritikus biztonságigényű adatok kezelése

Map reduce

- Hadoop – nagy adatmennyiségek tárolására és kezelésére használt noSQL rendszer
- Adattárolás struktúrálatlan
- Lekérdezés
  - Módja: Map-Reduce
  - Két függvény (Map és Reduce függvények)
    - Igény szerint szükséges implementálni

Map-Reduce


Shuffle
Sort + Send
Merge
Split 0
Split 1
Split 2
Split 3
Split 4
Map
Map
Map
Key-1 : Value-1
Key-2 : Value-2
Key-1 : Value-3
Key-2 : Value-4
Key-2 : Value-5
Key-1 : Value-6
Key-1 : Value-1
Key-1 : Value-3
Key-1 : Value-6
Key-2 : Value-2
Key-2 : Value-4
Key-2 : Value-5
Reduce
Reduce
Part 0
Part 1
Input files
(on HDFS)
Intermediate files
(on local disks)
Output files
(on HDFS)

Map-Reduce

- **Lépései**
- Adathalmaz szétszórása mapperek között
- Mapperek
  - Map: adatelemek csomópontokhoz rendelése és feldolgozása →részeredmény, (kulcs, érték) párok
- Azonos kulcsú elemek azonos reducer-hez
- Reducerek
  - Reduce: csomópontok részeredményeinek feldolgozása →végeredmény

Map-Reduce

- Példák:
  - Szavak megszámolása szövegben
    - Szöveg random feldarabolása mapperek között
    - Minden mapper előállít (szó, darabszám) párokat minden olvasott szóhoz
    - Minden mapper szó, mint kulcs alapján szortíroz a Reducerek között
      - kutya → 1. reducer, macska → 2. reducer, teknősbéka → 3. reducer
    - Minden reducer kap egy adott szóhoz több darabszámot, amiket összead
      - Pl. 1. reducer: (kutya, 3), (kutya, 4), (kutya, 2) → (kutya, 9) az eredmény egy része
  - Adott nevű emberek átlagéletkorának kiszámolása
  - Szórás kiszámolása
  - Havi legmagasabb hőmérséklet megtalálása

Blockchain és Bitcoin

- Blockchain
  - Adattárolási technológia
  - Teljesen elosztott - egyenrangú felek
  - Biztonsági kérdéseket is kezel
- Bitcoin
  - Blockchain fő használati területe
- Bitcoin vs Blockchain
  - Bitcoin – kriptovaluta
    - Vehető, bányászható
  - Blockchain – mögöttes tárolási technológia
    - A Bitcoin átutalását teszi lehetővé A-ból B-be
  - Nem összekeverendő!

Bitcoin motivációja – utalás sebessége

- Belföldön
  - Van, hogy lassú
- Pénz átvitele Magyarországról Új-Zélandra?
  - Nemzetközi utalásnál még lassabb

Bitcoin motivációja – a bank

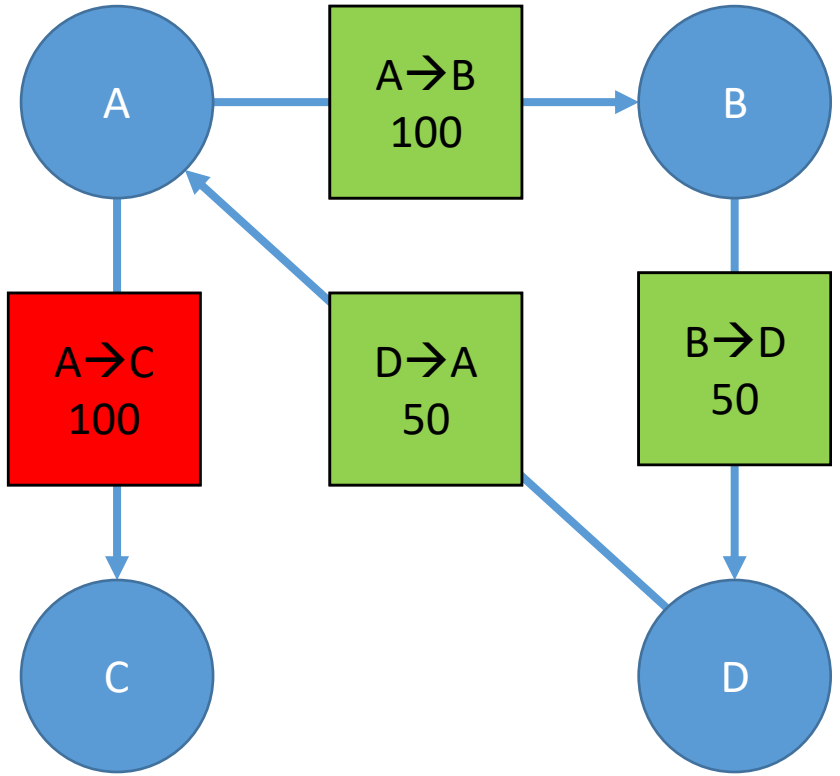
- Jelenlegi átutalás – közvetítővel (bank)
- Problémák?
  - Bizalom a köztes szereplőben
  - Drága – Jutalom a köztes szereplőnek ($$$)
  - Centralizált - SPOF
  - Támadható – POS terminál - ügyféladatok
  - Mi van, ha kiveszem minden pénzemet?
- Célok?
  - Centralizált helyett legyen elosztott!
  - Ne legyen köztes szereplő!

Bitcoin alapötlete

- Satoshi Nakamoto
  - 2008 októberében írt cikk
- NINCS bank
- Helyette?
  - Közös főkönyv (ledger)
  - Átutalások naplója
  - NINCS bankszámla

Főkönyv - példa

- Példa: Tfh. A-nak eleinte van 100 BTC-je
- Mindenkinek átküldjük a tranzakciókat
  - Hálózatban terjed
  - Bárki leellenőrizheti
  - Bankszámla **nincs** – nincs egyenleg
- Probléma – privacy
  - Mire költöm a pénzemet?
  - Mivel nyilvános, mindenki tudja?

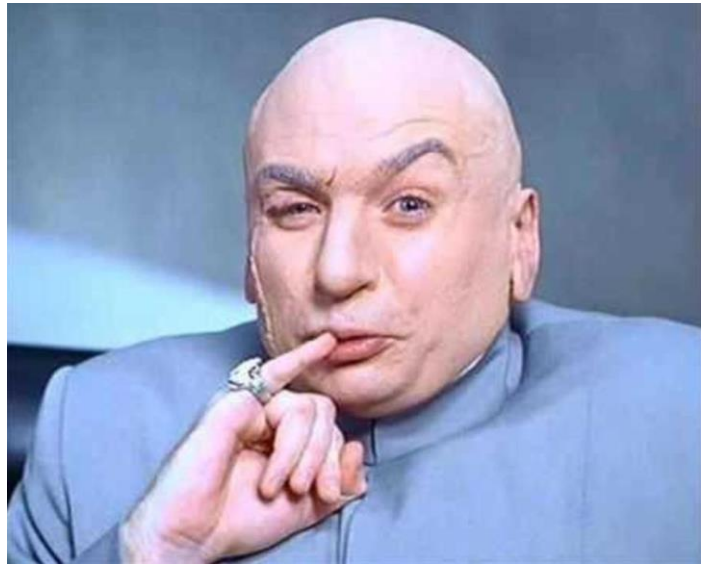


Privacy

- Eddig:
  - Számlaszám – nyilvános
  - Egyenleg és tranzakciók – titkos
- Mostantól?
  - Identitás – titkos
  - Tranzakció – nyilvános
  - 66342bca83d utal 1 BTC-t 9fd8874234-nek

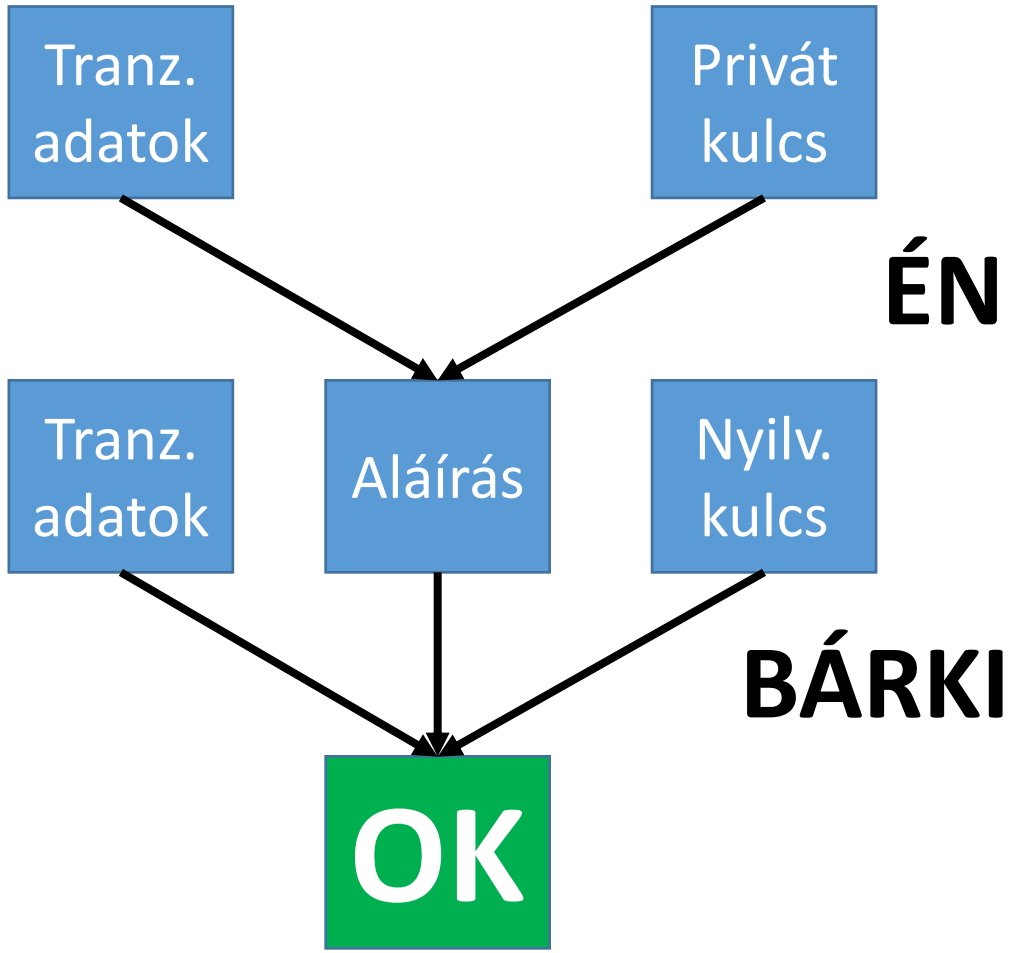
Támadás

- Probléma
  - Nincs köztes szereplő
  - Nincs személyazonosságom
  - Létrehozhatok egy tranzakciót, ahol magamnak utalok?
  - Bill Gates → Én: 1M USD ???



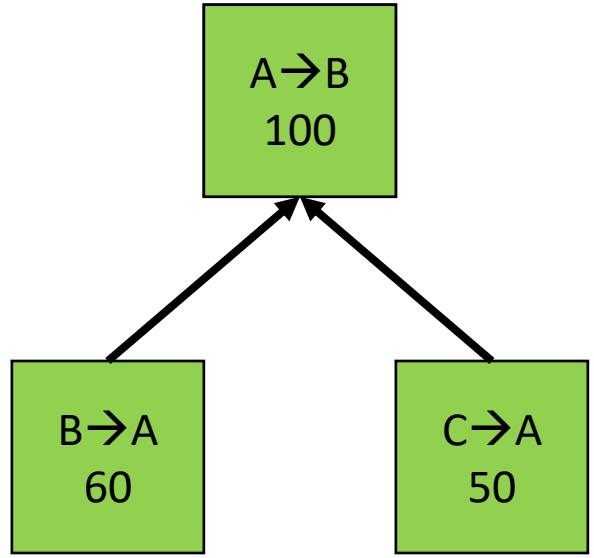
Megoldás – digitális aláírás

- Két kulcsom van (ahogy minden más felhasználónak)
  - Nyilvános – mindenki ismeri
  - Privát – csak én ismerem
  - N(P(x))=x
- **Ellenőrizhető, hogy csakis a jogosult küldhette**
- A lehetséges kulcsok nagy száma miatt gyakorlatilag lehetetlen a kulcsegyezés.
- Irodalom
  - Katona-Recski-Szabó:
    A számítástudomány alapjai
  - Buttyán-Vajda:
    Kriptográfia és alkalmazásai



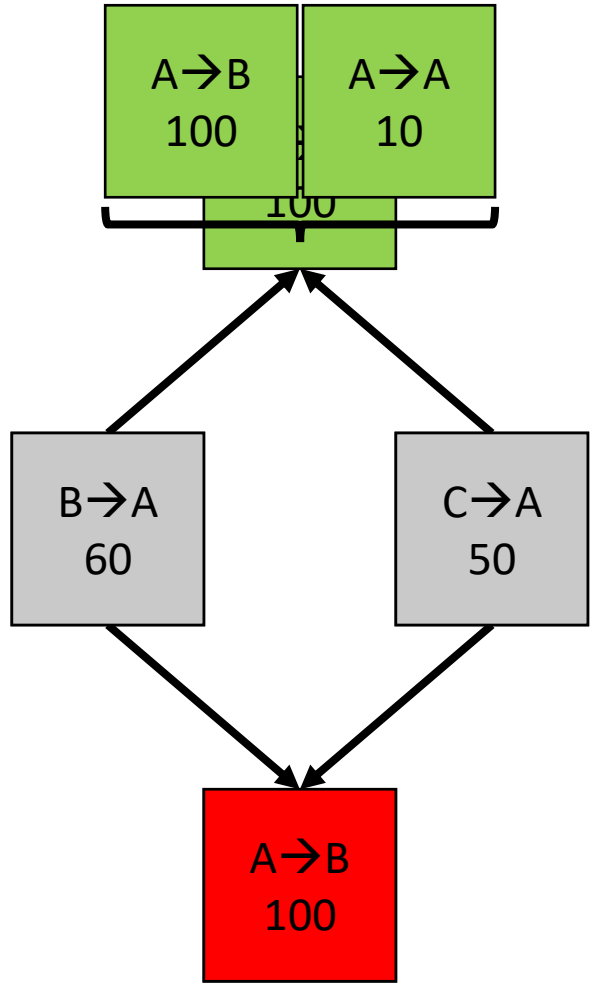
Van-e rá pénzem?

- Nincs bankszámla – hol látszik a fedezet?
  - A tranzakciókból
- Tranzakciók visszakövetése
  - vö. relációs adatbázis **helyett** redo log
- Nem bonyolult?
  - Nem! Tranzakciók megjelölése
  - Telepítés után egy ellenőrzés (24 óra is lehet)



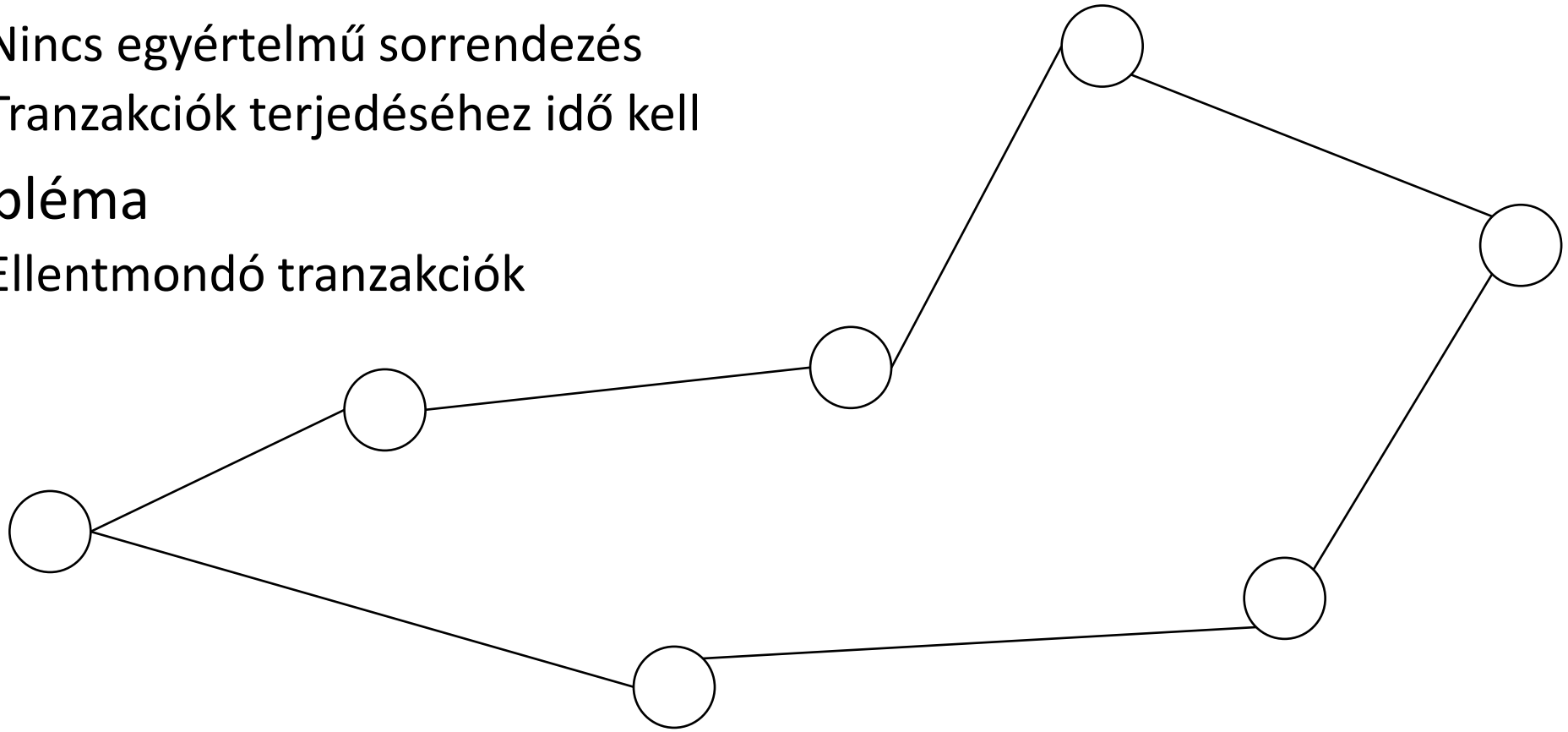
Probléma – dupla fedezet

- Tegyük fel, hogy kétszer jelölünk ki valahány tranzakciót fedezetként
- Megoldás?
  - Elköltöttnek jelölés
  - Többször nem használható fel.
- Egyéb probléma?
  - 60+50>100
  - Hová tűnik a pénz?
- Megoldás?
  - Fedezet=költés – utalhat magának
  - Később ugyanúgy használható fedezetnek.



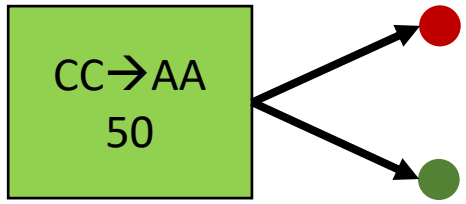
Támadás – kétszeri költés

- Adottság
  - Elosztott rendszer
  - Nincs egyértelmű sorrendezés
  - Tranzakciók terjedéséhez idő kell
- Probléma
  - Ellentmondó tranzakciók

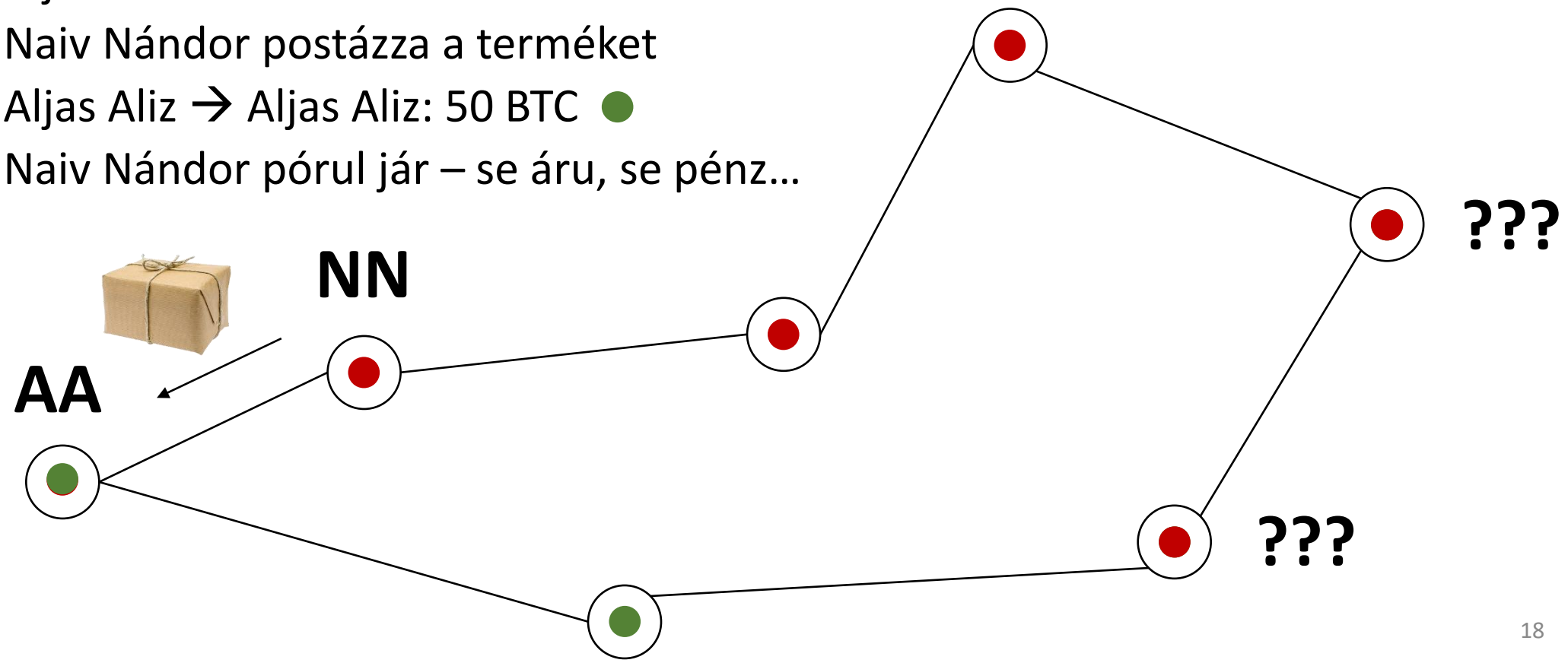


Támadás – kétszeri költés

Egy fedezet – két tranzakció



- Visszaélés
  - Aljas Aliz → Naiv Nándor: 50 BTC
  - Naiv Nándor postázza a terméket
  - Aljas Aliz → Aljas Aliz: 50 BTC
  - Naiv Nándor pórul jár – se áru, se pénz…

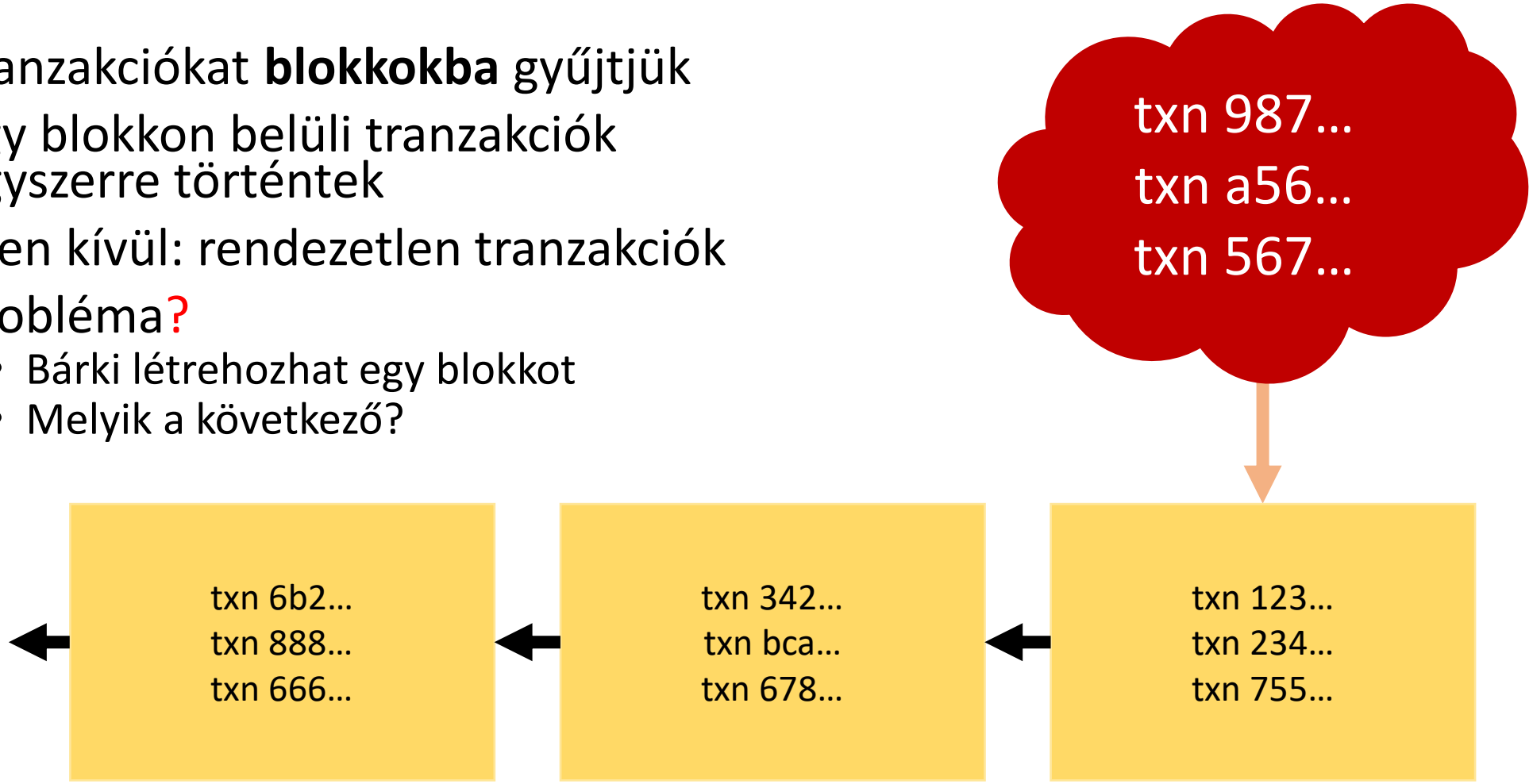


Támadás – kétszeri költés

- Probléma
  - Ellentmondó tranzakciók
- Visszaélés
  - Aljas Aliz két tranzakciót indított, egyet Naiv Nándornak, majd egyet magának is, ugyanazon fedezet alapján.
  - Ellentmondó információ miatt (melyik tranzakcióé a fedezet?) nem verifikált a NN-nak való utalás (persze a másik sem), de NN már elpostázta a terméket.
- Megoldás?
  - Globális rendezés

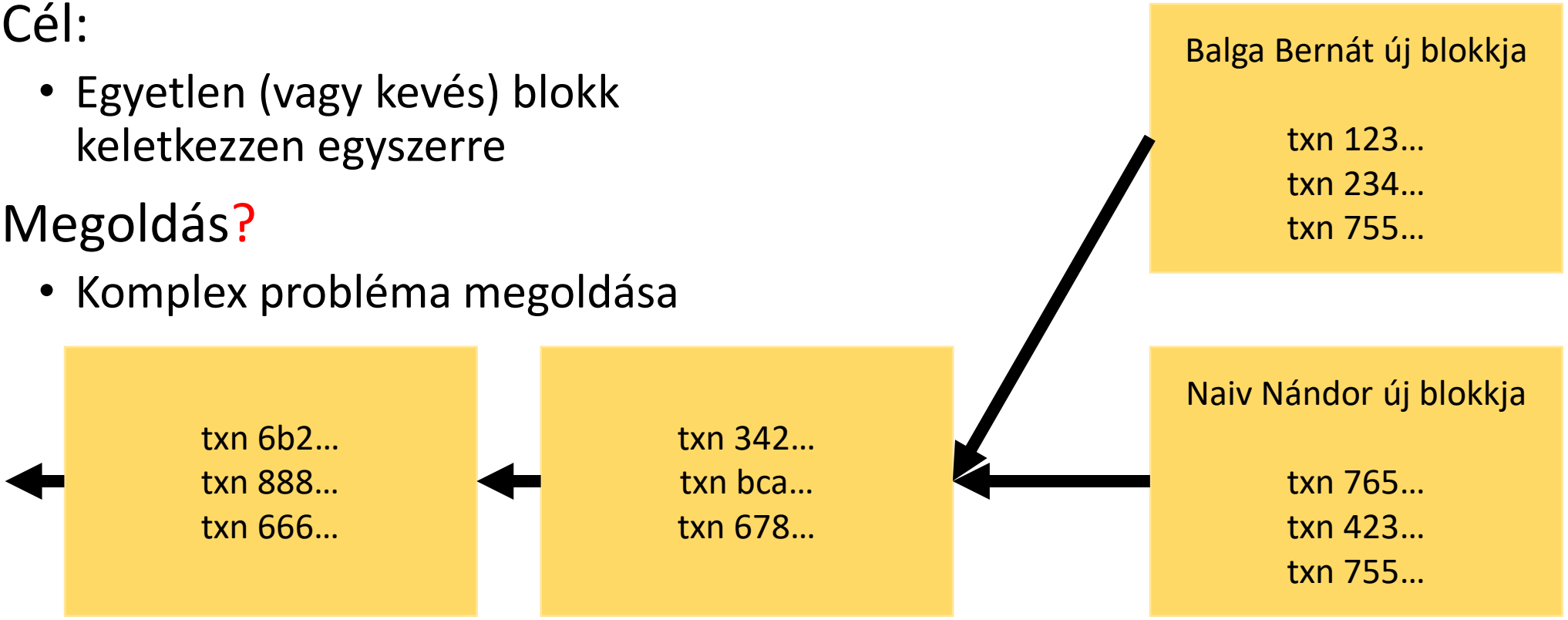
Globális sorrendezés – Blockchain

- Tranzakciókat **blokkokba** gyűjtjük
- Egy blokkon belüli tranzakciók egyszerre történtek
- Ezen kívül: rendezetlen tranzakciók
- Probléma?
  - Bárki létrehozhat egy blokkot
  - Melyik a következő?



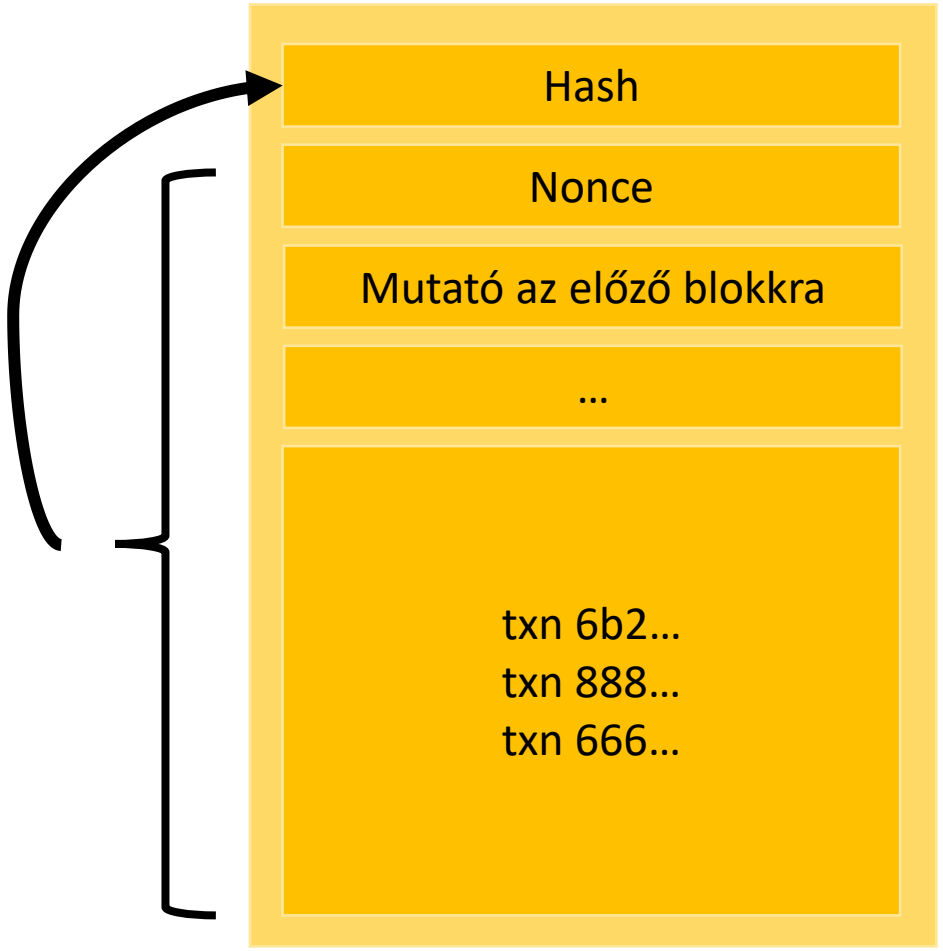
Globális sorrendezés – Blockchain

- Cél:
  - Egyetlen (vagy kevés) blokk keletkezzen egyszerre
- Megoldás?
  - Komplex probléma megoldása



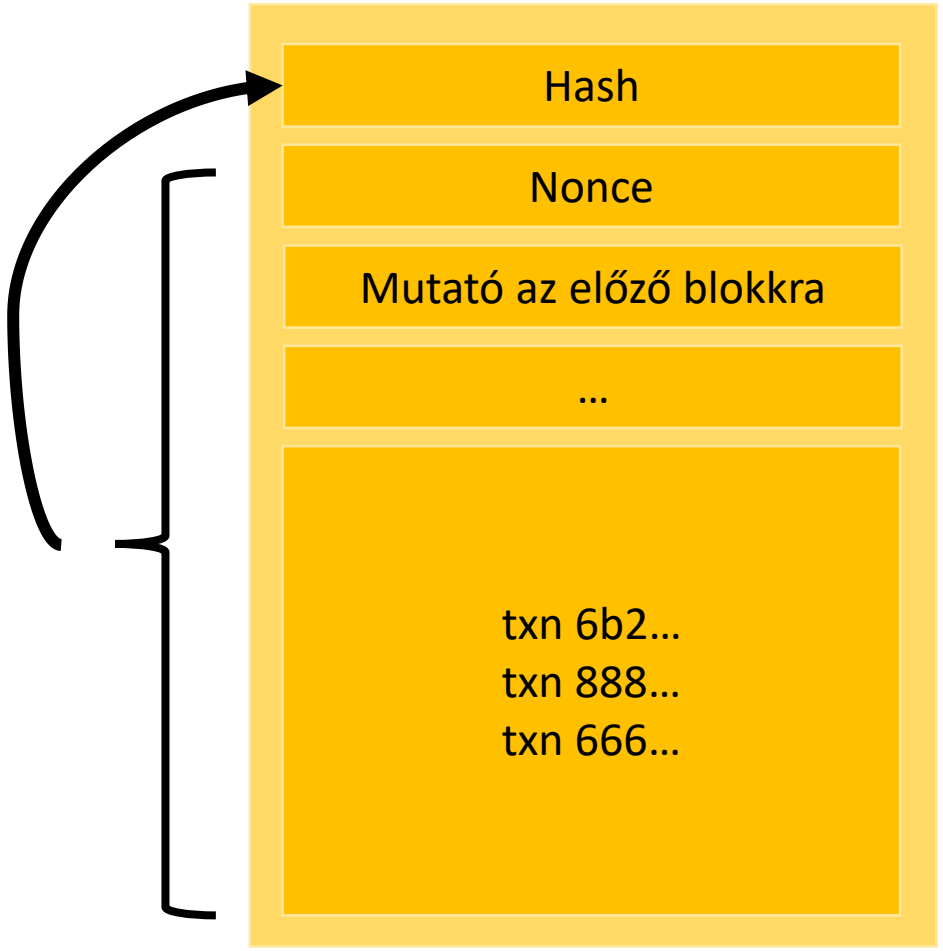
Blokklétrehozás ára – proof of work

- Komplex probléma
  - A blokk tartalmából **adott mintára illeszkedő** hash kiszámítása.
- Nonce
  - Blokk egy mezője
  - Szabadon választható értékű
- Hash
  - Blokk egy mezője
  - Meghatározott hosszú 0-sorozattal kezdődik
  - Kiszámítása:
    - H(blokk tartalma (nonce is)) == 0000000..?
    - Ha nem, nonce módosítása, és újra
    - Nehéz feladat előállítani
    - Könnyű ellenőrizni



Blokklétrehozás ára – proof of work

- Verseny
  - Ha megtaláltam a megfelelő nonce értéket, nyertem
  - Magas jutalom
- **Bányászat**
- Új blokk 10 percenként jön létre
  - Kb. ennyi idő kell a számításhoz
  - Hagyományos számítógépnek → több év!
- 10 percenként „zárás”
  - Az új blokk létrejöttével

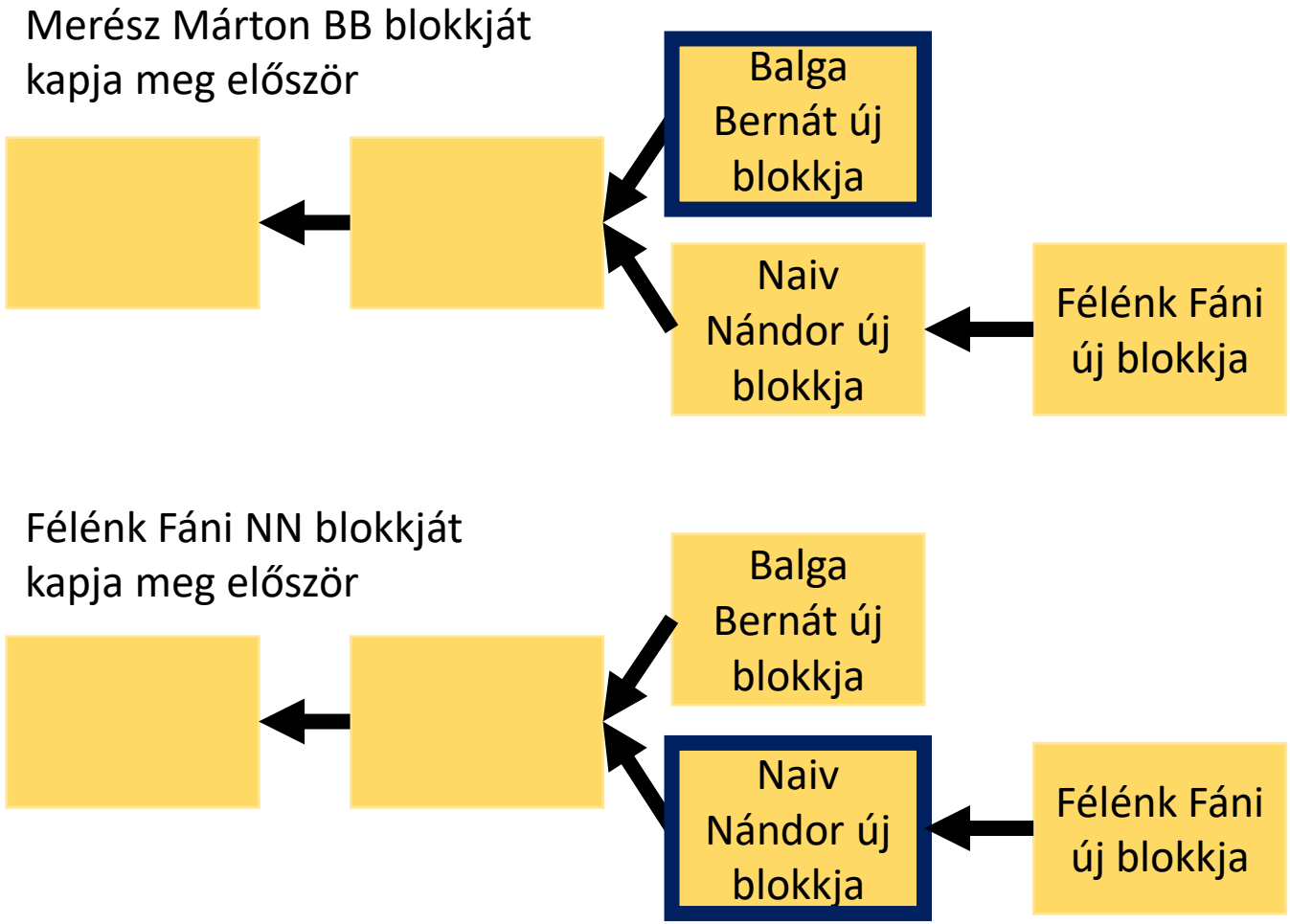


Hash funkciói

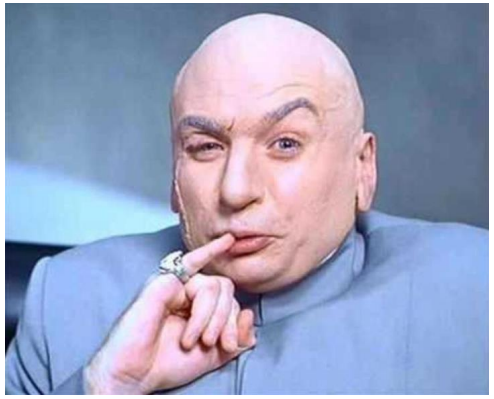
- Nehéz probléma megoldásának bizonyítéka
- Előző blokk mutatója
- Következmény?
  - Tfh. Valaki átírja egy korábbi blokk egy tranzakcióját
  - Tfh még a megfelelő hash-t is megtalálná az adott blokkhoz
- Nem teheti meg!
- A hash a tejes láncot védi.
  - Tartalmazza a blokk lenyomatát, ezen belül
  - Az előző blokk hash-ét…
    - …ami tartalmazza azon blokk lenyomatát és
    - A megelőző blokk hash-ét
    - Tehát az egész lánc lenyomatát

Probléma – több blokkzárás egyszerre

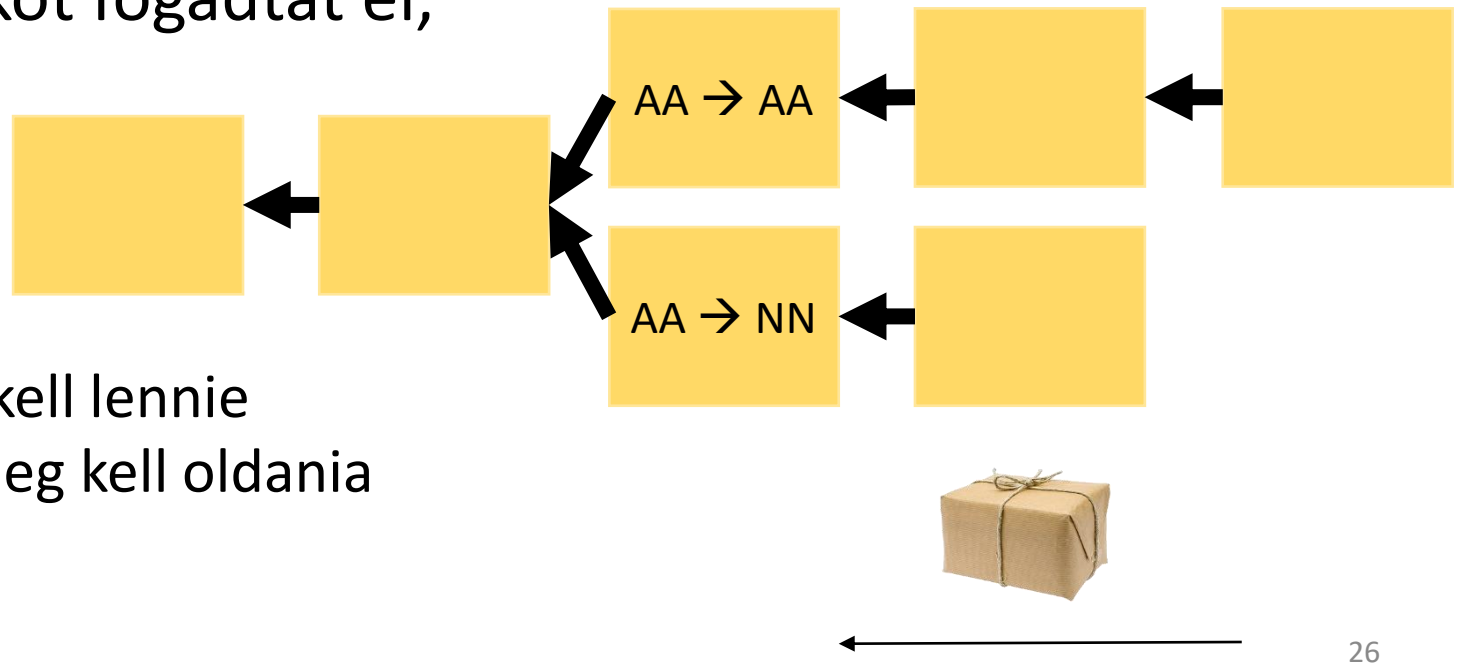
- Több bányász találja meg a blokkjelöltjének hash-ét
  - BB és NN egyszerre
- Valószínűtlen, de néha megtörténik
- Terjed a hálózatban
- Melyik az igazi?
  - Amelyiket először kaptam meg, arra építem a következő blokkomat
  - Felhasználónként eltér
- Több ág?
- Következő zárásig
- Tfh. FF zárja elsőként a következő blokkot
  - Elterjed
  - NN ága lesz a nyerő!
  - Stabilizálódik a BC
- **Nyertes ágban nem szereplő tranzakciók → Rendezetlen tranzakciók**



Támádás – kétszeri költés – ismét



- Tfh. Aljas Aliz elutalja a pénzt Naiv Nándornak
- Naiv Nándor vár, míg a tranzakciója bekerül egy blokkba
- Naiv Nándor postázza a terméket
- Aljas Aliz alternatív blokkot fogadtat el, új ágon
  - AA → NN utalás helyett
  - AA → AA utalás
- Lehetséges?
  - AA ágának hosszabbnak kell lennie
  - AA-nak több blokkot is meg kell oldania



Támadás – kétszeri költés – ismét

- Aljas Aliz esélyei
  - Csekélyek
  - A világ ellen versenyez
  - A világ számítási kapacitásának fele kell,
    - hogy 0,5 valószínűséggel győztesként számoljon ki egy blokkot
    - hogy 0,25 valószínűséggel győztesként számoljon ki két egymást követő blokkot
    - …
  - Nem éri meg.
- Viszont:
  - Újabb blokkok jobban támadhatók
  - Több blokkot érdemes várni az utalás ellenszolgáltatása előtt (postázás előtt)

Záró kérdések

- Honnan jön a bitcoin?
  - Bányászat
    - 2020. május 12, 10:42:07 UTC-kor 6,25 BTC-re csökkent 12,5 BTC-ról
    - Feleződik négyévente
    - Előre ismert a forgalomban lévő BTC-k maximális mennyisége
  - Tranzakciós díjak
    - Jelenleg nem jellemző, többet ér a nyeremény
    - Később felértékelődhet a szerepe

Záró kérdések

- Mi értelme a bányászjutalomnak?
  - Nem „nyomtatott pénz”, mivel munka van mögötte.
  - Elrettentő erő a csalástól
- Mi fán terem a bánya?
  - „Haverom azt mondja, bányászik” Komolyan mondta? Felépített egy saját bányászerőművet? Honnan van ennyi pénze? Hol éri meg? Egyedül számol ki blokkokat? Egyedül nyer 6,25 BTC-t? → NEM(valószínű)!
  - Mining pool – lehet csatlakozni, teljesítménnyel hozzájárulni. Befektetett munka arányában részesülünk a jutalomból.

Záró kérdések

- Hardver
  - Sima PC → VGA → célhardver
  - Top 500 szuperszámítógép kapacitásának 50000-szerese
    - De másra nem használható
    - Teljesítménymérő – Exahash/sec

Hol termett az első Bitcoin?

- Genesis block
  - 2009. jan. 3-i Times címlap szalagcímét tartalmazta
  - 50 BTC-s jutalom a 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa címre ment

```
00000000   01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD  7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3  88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49  FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00  00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF  FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54  69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39  20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62  72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62  61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73  FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04  67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10  5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6  49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE  5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷°..W
00000110   8A 4C 70 2B 6B F1 1D 5F  AC 00 00 00 00           ŠLp+kñ._¬....
```


THE TIMES

Eat Out from £5

More than 900 great restaurants, including four Gordon Ramsay favourites from £15

Israel prepares to send tanks and troops into Gaza

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

Michael Sheen Frost, Nixon and me

Working mums So that's how she does it

Detox in style The best spas on the planet

Salmon Rushdie I Won't Marry Again

Giant Killing? Guide to the FA Cup Third Round

Nyitott problémák – No Free Lunch (NFLT)

- Skálázhatóság
  - Új belépőkkel tranzakciók száma nő
  - Főkönyv mérete elszabadulhat →
- Méret
  - 150 – 300 GB szabad hely kell jelenleg
  - 2018. március 18-án 161371 MB
  - 2019. szept. végén 242,39 GB
  - 2020. április 26-án ~ 270 GB
  - 2021. április 13-án 331,07 GB
  - 2022. április 22-én 402,08 GB
  - 2023. május 8-án 478,91 GB
  - https://bitcoin.org/en/bitcoin-core/features/requirements
  - Bitcoin Blockchain Size (ycharts.com)
- Tőzsdei sebezhetőség
  - 2018 eleje – árfolyamfeleződés
  - 2020 ősz- 2021 tavasza - árfolyamötszöröződés
  - „bizalom…” a BTC-ben
- Az anonimitás olykor hátrány
  - Terrorszervezetek kedvelt fizetőeszköze
- Egy megoldás a méretproblémára – Pruning
  - https://steemit.com/bitcoin/@sweecee/how-to-lower-bitcoin-and-other-cryptos-disk-space-by-using-pruning-command
- Irdatlan környezetterhelés
  - több tízmillió tonna CO2 csak az USÁ-ban