Blockchain — van ennek értelme?

Megkerülhető a BC technológia?

Vágujhelyi Ferenc

Az információkezelés új módszere

- mikor motivált államok közötti nemzetközi együttműködést? (European Blockchain Partnership)
- mikor hozott új szabályokat az adórendszerben (kripto-eszközök)?
- mikor hozott jogalkotási kényszert a hitelesség és bizonyító erő szabályozásában?
- mikor vetette fel új szabályok szükségességét a kötelmi jogban (okosszerződések)?
- mikor tett lehetővé olyan jogi vagy gazdasági tranzakciókat, amelyek módosítására senkinek sincs hatalma?

Ez a technológia korábban nem létező társadalmi kérdéseket vetett fel.

Pénz

Ingatlan

Részvény

Szerzői jog

Gyémánt

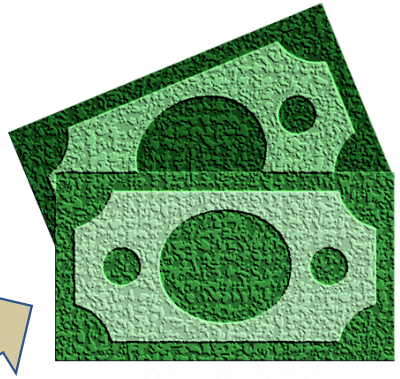
Értékpapír

✅	1.	Zárt rendszerben	Csak a rendszeren belül hiteles (pl. bankszámla)
✅	2.	Elektronikusan hitelesítve	A hitelesség a bizalmi szolgáltatón alapul
?	3.	Decentralizáltan	Bizalom nélkül

A blockchain születése

Absztrakciós fejlődés

A pénzérme hordozza az értéket



A bankjegy reprezentálja az értéket

Egy felügyelt banki rendszerben elektronikus jel reprezentálja a pénzt.

Matematikai protokoll felügyeli az elektronikus jelben reprezentált értéket

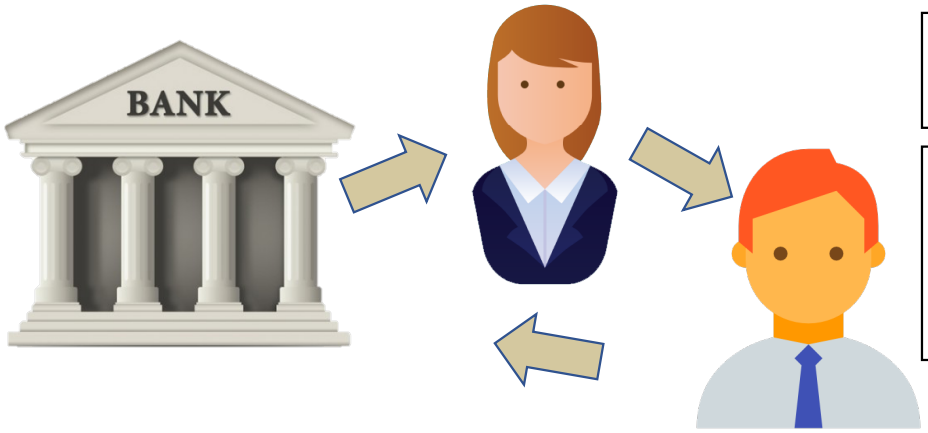
Technológiai fejlődés

Kriptopénz

A külső tekintélytől független elektronikus pénzzel szemben ezért a következőket várták el:

- tisztán a használók közötti —pénzintézet nélküli— kapcsolaton alapuljon (purely peer-to-peer),
- a rendszer legyen teljesen decentralizált (mindenki egyenrangú),
- az emissziót (pénzkibocsátást) a protokoll végzi; az új „e-bankjegy” első „tulajdonosságára” a rendszer működtetőinek annak arányában legyen esélye amennyi munkát a rendszer működtetésébe befektettek,
- mindenki csak a saját pénzét költheti,
- visszamenőleg ne lehessen tranzakciót módosítani,
- ugyanannak a pénznek a dupla elköltése ne teremtsen új pénzt,
- a résztvevők közötti eltérő adatok esetén a protokollt betartók jussanak konszenzusra az érvényes adattartalmat illetően,
- a protokoll a kötelező, a szoftver nem (a blockchain maga a protokoll, a szoftverek valósítják meg).

Egyszerű kriptopénz előállítása (aláírt váltó-szerű modell)




```
bankjegyNo874191.txt: Ez a 874191 sorszámú
elektronikus bankjegy 100 egység értékű.
```

```
gpg --clearsign bankjegyNo874191.txt
gpg: using
"C0F37557DB1735CFA736AEC4CC748F008639301C"
as default secret key for signing
```

Az eredmény:

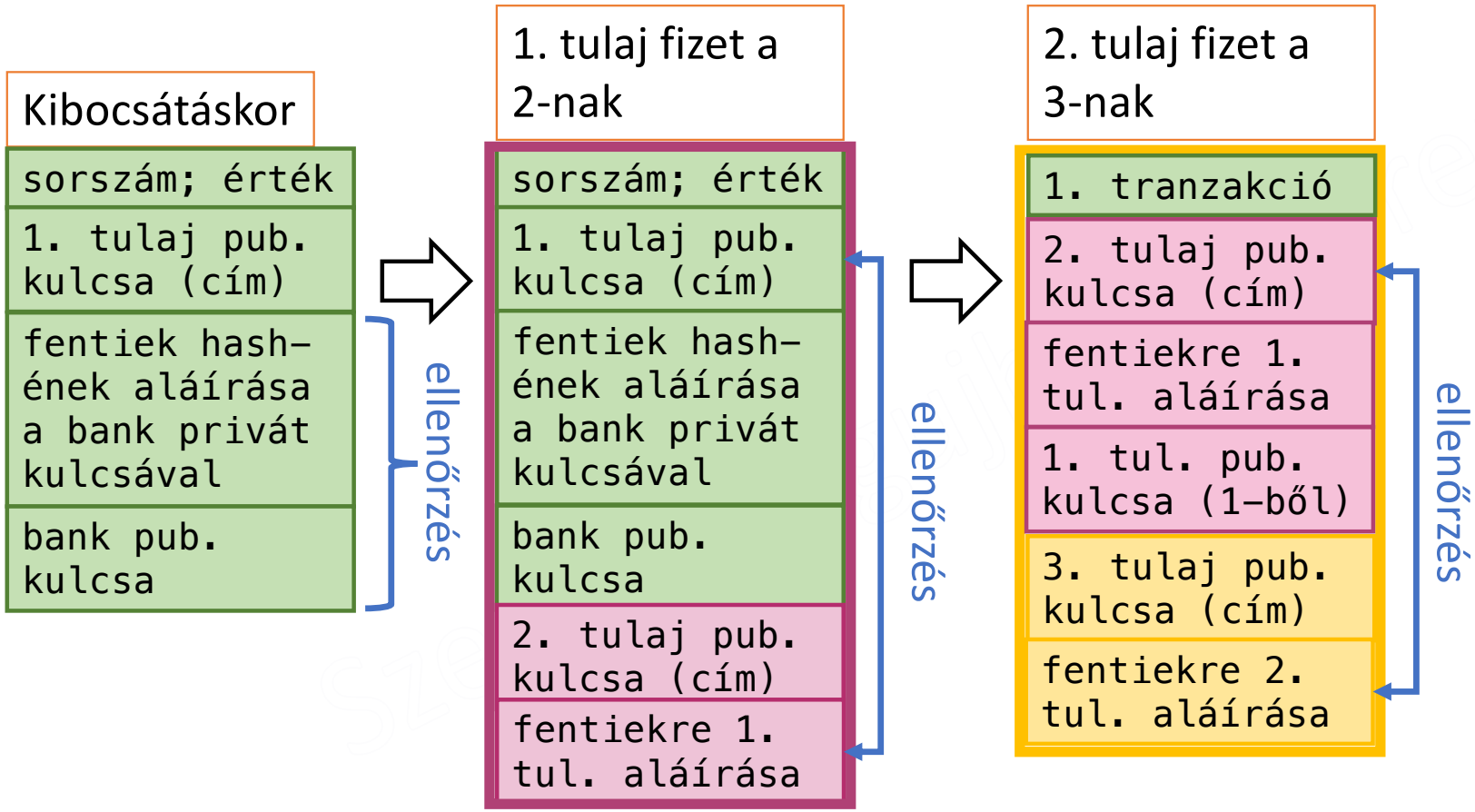
```
bankjegyNo874191.txt.asc
```

- A pénzt csak a bank tudta előállítani.
- Hitelességét a bank nyilvános kulcsával bárki ellenőrizheti.
- Másolható, ezért a bank annak a követelését ismeri el, aki először mutat be egy példányt,
- ezért bárki használhatja akinek van másolata,
- így mindig azonnal be kell váltani!

Csak a közvetlenül a banktól kapott pénz esetén biztos, hogy még nem váltották be!

Egyszerű kriptopénz használata (csak a címzett használhatja)

Eredeti kibocsátás: `bankjegyNo874191.txt` használatával



A ⇨ jel itt közzététel is lehet!

Ellenőrzés: az aláírás (cím) publikus kulccsal való dekódolása a tranzakció hash-kódját adja?

a) Ha a másnak címzett pénzt nem a címzett írja alá: nem.

b) Ha átírom a cím kulcsot a sajátomra, az előző aláírás hibás lesz!

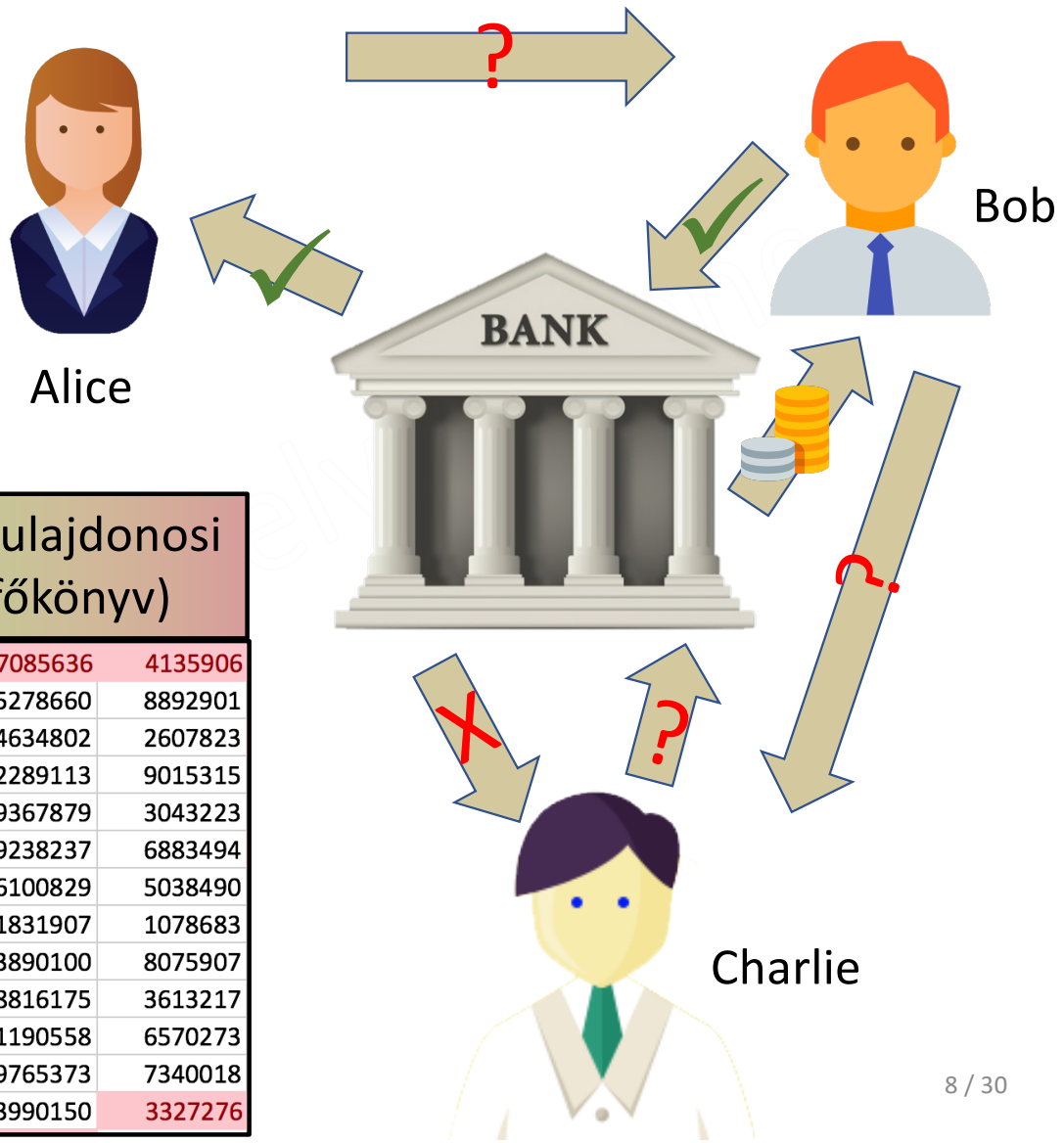
A dupla költés megoldása

- A dupla költés ellenőrzéséhez a banknak be kell jelenteni minden tranzakciót!
- A teljes rendszer hitelességét a bank adja (hiányosság)!

A tulajdonosi lista azzal egyenértékű, hogy a bankjegy elfogadója az átvett bankjegyet a banknak elküldi, aki egy nyilvános főkönyvben azt közzéteszi, ha a bankjegy az utolsó ismert állapotából szabályos költésekkel jutott az aktuális állapotába.

A lekérdezés után adott ideig a lekérdezőnek zárolja a pénzt.

Hiteles tulajdonosi lista (főkönyv)		
1481117	7085636	4135906
4219407	5278660	8892901
5522450	4634802	2607823
1158536	2289113	9015315
6189812	9367879	3043223
4844390	9238237	6883494
3969176	6100829	5038490
9934767	1831907	1078683
9672902	3890100	8075907
8680019	8816175	3613217
7377358	1190558	6570273
2584720	9765373	7340018
2223741	3990150	3327276



Minek a bank?

1. A kibocsátást végzi.

2. Üzemelteti a főkönyv szolgáltatást.

3. Ellenőrzi, hogy a főkönyvbe csak az utolsó ismert állapotból szabályos tranzakciókkal (költésekkel) módosuló bankjegyek (vagy pénzérmék) kerüljenek.

Legyen a főkönyv vezetéséért jutalom!

Mindenki vezethet főkönyvet aki akar!

Erre bárki képes!
Pl. aki elfogadja az érmét.

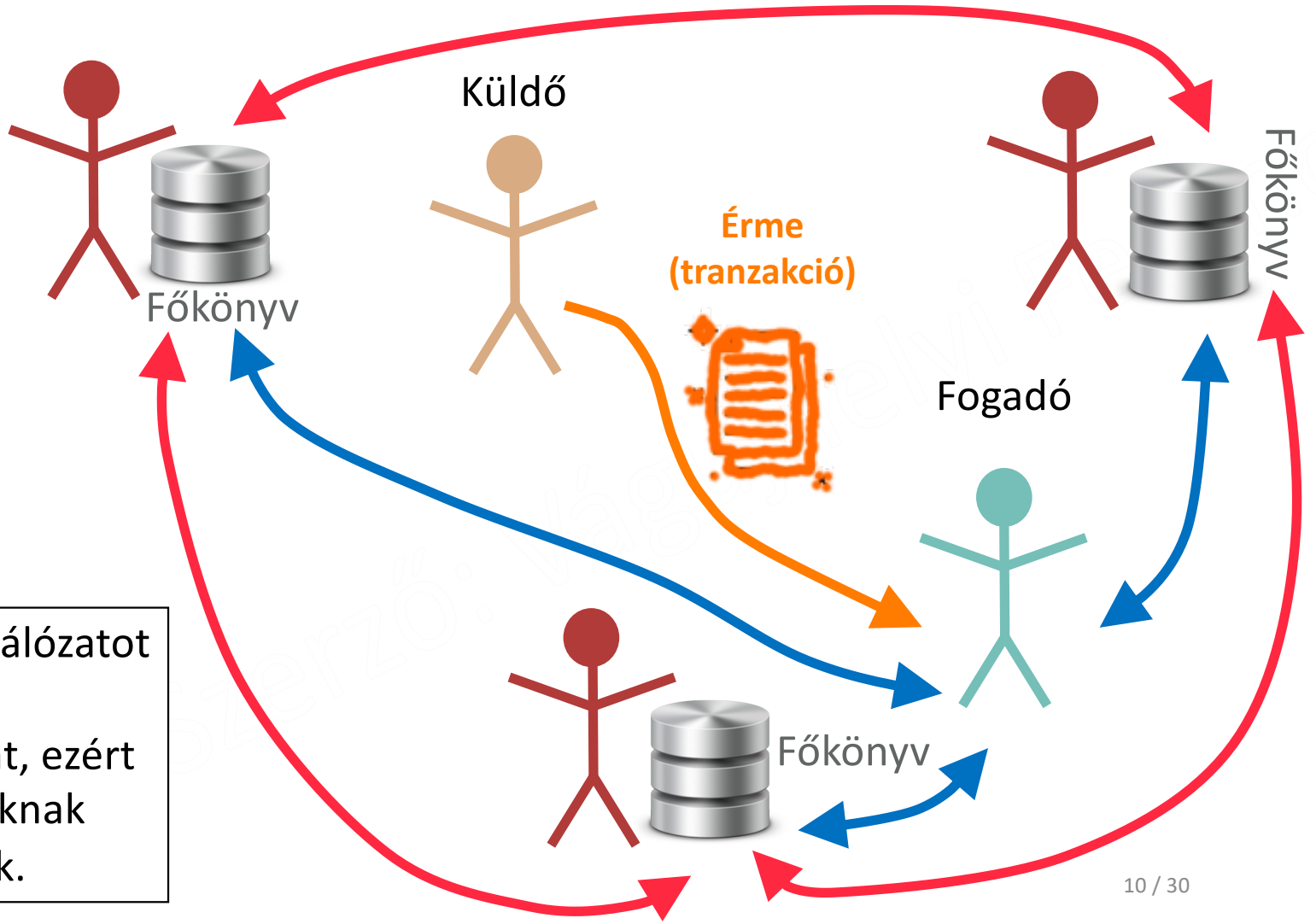
A központ nélküli főkönyv (amiben pénzt hitelesítünk!)

Tranzakció adatának átadása:

Főkönyvet vezetők értesítése:

Főkönyvek közötti szinkron:

A főkönyvet vezetők egy hálózatot létrehozva folyamatosan szinkronizálják az adataikat, ezért őket hálózati csomópontoknak vagy node-oknak nevezzük.



Mit nem oldottunk meg?

1. Az emissziót (érme kibocsátást): a node-ok az érmék szabályosságának vizsgálatánál végső soron a kibocsájtó aláírásáig kell, hogy ellenőrizzék a tranzakciókat. Az érme használóinak az aláírását csak technikailag kell ellenőrizniük. A kibocsátó aláírásánál viszont azt is vizsgálni kell, hogy a kibocsátó szervezet elismeri-e sajátjának! A bankot, illetve aláírásának hitelesítőjét (CA) tekintélyként fogadjuk el. A CA a rendszeren kívüli szabályok alapján működik. A bank a rendszeren kívüli szabályok alapján teremt új pénzt.

2. Ugyanannak a pénzérmének a dupla elköltése nem teremt új pénzt, sőt az érintett sorozatszámú pénzt „további intézkedésig” kiveszi a forgalomból. Viszont nem biztosítunk módszert arra vonatkozóan, hogy miként alakítható ki konszenzus abban, hogy a több tranzakcióból melyik az érvényes. A hibalista ténye az ellenmondás rögzítése a főkönyvben. Így az ezzel kapcsolatos döntést megint a tekintélyre kell hagynunk, aki a rendszeren kívüli szabályok alapján hoz döntést.

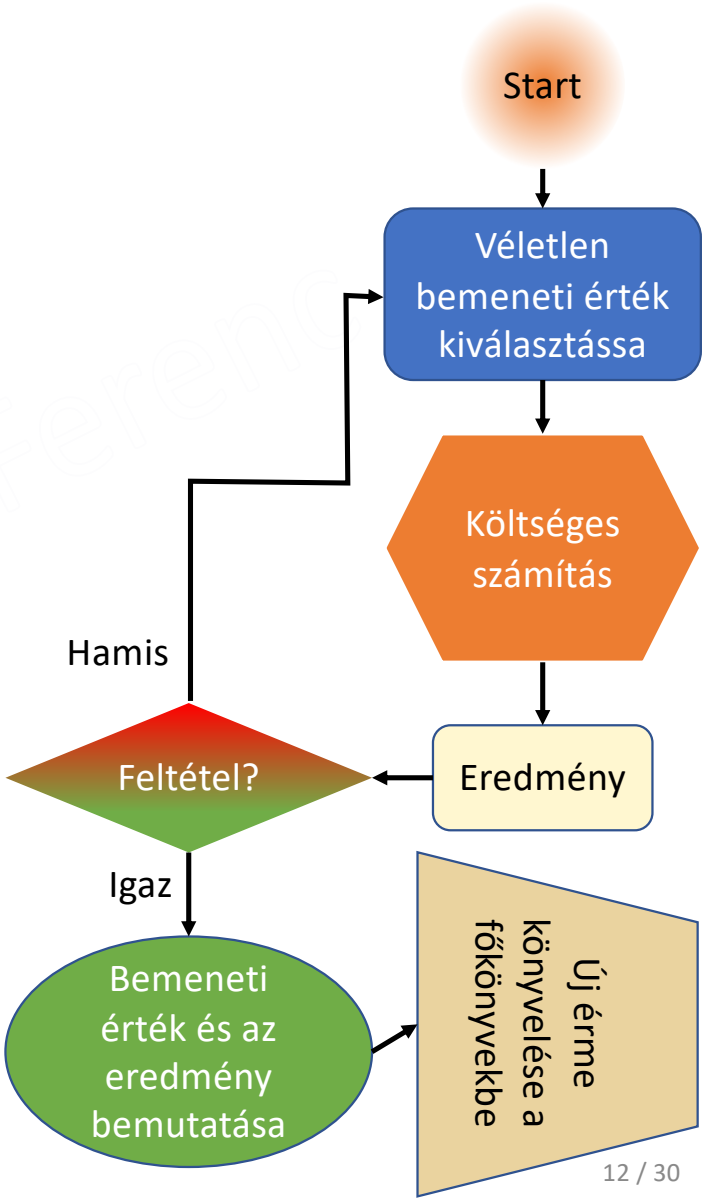
A fenti problémák megoldása teremtette meg a blockchaint.

A kriptopénzt is bányásszuk!

kriptopénz

- Erőfeszítéssel lehessen megteremteni!
- Ne legyen túl sok (infláció)!
- Ne legyen túl kevés (más veszi át a szerepét).

A kriptopénznél a digitális térben mozgunk. A befektetett munkát itt sok számítás elvégzése jelentheti. Ez automatikusan időt vesz igénybe. A véletlen tényezőt az jelenti, hogy ha a számítás eredménye nem felel meg valamilyen tulajdonságnak, akkor más bemenő paraméterrel újra el kell végezni.



A számítást csak egy irányba (előre) szabad tudni elvégezni, különben a jó eredményből számolok bemeneti értéket!

Függjön a siker a hash (lenyomat) függvény eredményétől!

1. A kriptográfiai hash-függvények kimenetére írjuk elő, hogy hány darab nullával kezdődjenek.
2. Ha nő a bányászok teljesítménye, azaz egységnyi idő alatt több pénz kerül forgalomba, növekedjen a feladat nehézsége: nőjön egyel a szükséges nullák száma.

Ezért:

1. Tíz percenként gyűjtsük blokkba a nekünk jelentett tranzakciókat!
2. A blokk mögé írjunk olyan adatot, amellyel együtt a hash-érték x db nullával kezdődik! Nem tudjuk, hogy mit kell odaírni. Az egyetlen megoldás a próbálgatás.

Ha pl. az a feladat, hogy a „Hello, world!” karakterlánc mögé rakjunk valamit úgy, hogy a kiegészített karakterlánc hash-kódja 16-os számrendszerben kezdődjön négy db. nullával. Ha 0-tól számokkal próbálkozunk, akkor láthatjuk, hogy a 4250-es próba sikeres lesz!

"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64 ✗

...1...2...3...4...5...6...7.....354...355...356.....799...800...801.....3477...3478...3479.....4249... ✗ .. ✗ .. ✗ .. ✗

"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 ✓

Decentralizált tranzakció nyilvántartás

Központi nyilvántartás nélkül nem vagyunk képesek a címzettek azonosítására!

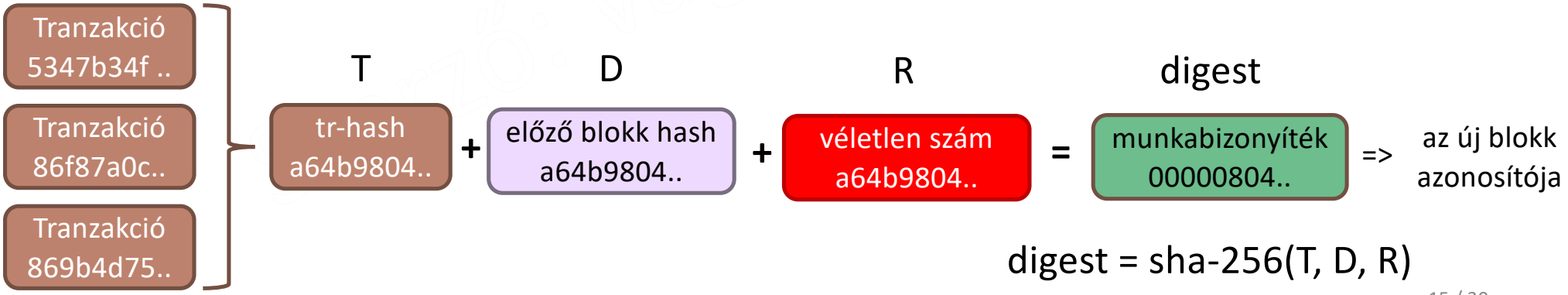
- a pénz elköltője csak bizonyítékot ad arról, hogy ő olyan dologgal rendelkezik, amivel csak a címzett rendelkezhet (de azt sem mutatja meg)!

sorszám; érték
1. tulaj pub. kulcsa (cím)
fentiek hash-ének aláírása a bank privát kulcsával
bank pub. kulcsa
2. tulaj pub. kulcsa (cím)
fentiekre 1. tul. aláírása

Saját korábbi kriptopénzünknél az érmékhez hozzáadott adatokban volt a tulajdonosok publikus kulcsa. Emlékezzünk: az azonosítás itt úgy történik, hogy aki az utolsó tranzakcióban megjelölt publikus kulcs privát kulcs párjával alá tudja írni a következő tranzakciót, csak az tudja elkölteni az érmét. Azt az egyetlen személyt, aki erre képes hívhatjuk tulajdonosnak.

A kriptovalutánál ki könyvelje a következő tranzakciót?

- Mindegyik node gyűjti a hozzá bejelentett tranzakciókat.
- Ha elég sok összejött, veszi a hash-kódjukat, hozzáteszi az előző blokk hash-kódját, majd addig próbál mőgé rakni egy véletlen adatsort (nounce), ameddig az ebből számolt hash nem kezdődik elég sok nullával.
- Aki sikeresen lezár egy blokkot, az a többieknek ezt bejelenti.
- Mindent azonosítson a hash-kódja! (az biztos, hogy egyedi)



A blokklánc

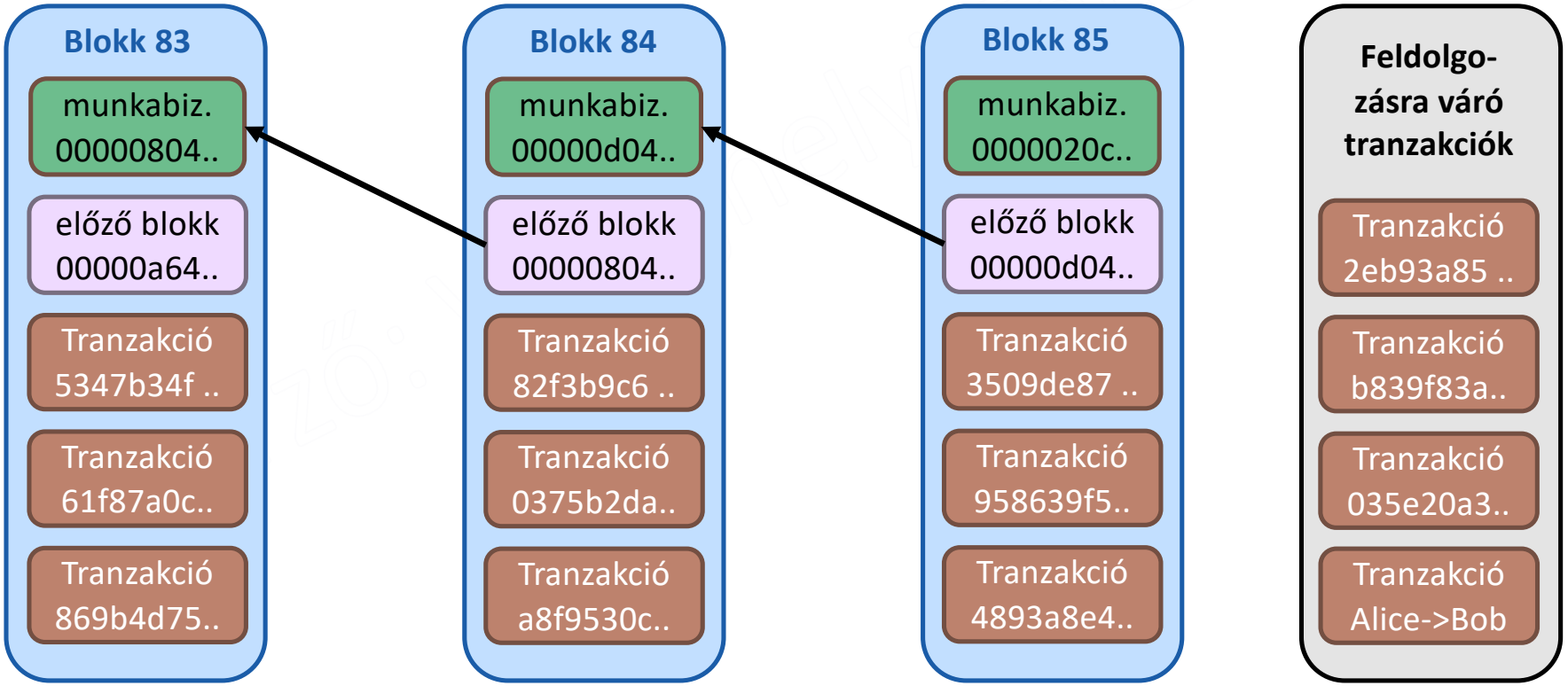
Tranzakció 5347b34f ..

Tranzakció 86f87a0c..

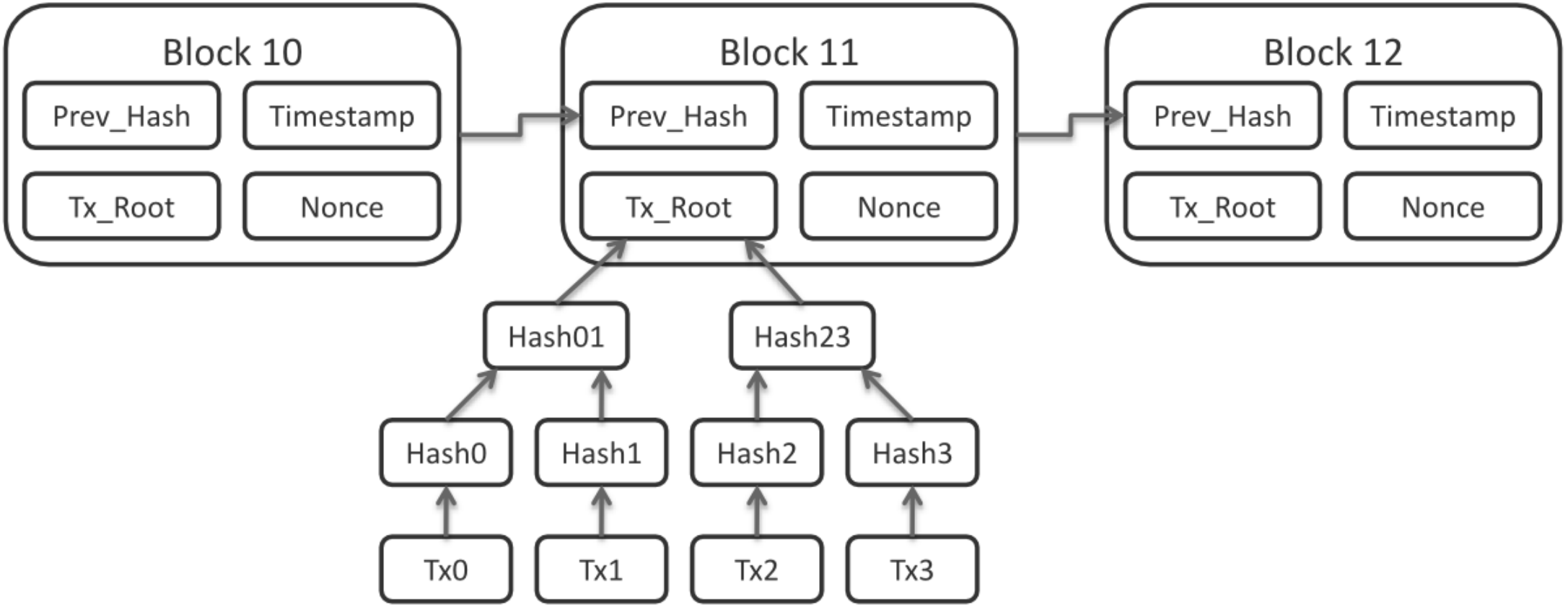
Tranzakció 869b4d75..

tr-hash a64b9804.. + előző blokk hash a64b9804.. + véletlen szám a64b9804.. = munkabizonyíték 00000804.. => az új blokk azonosítója

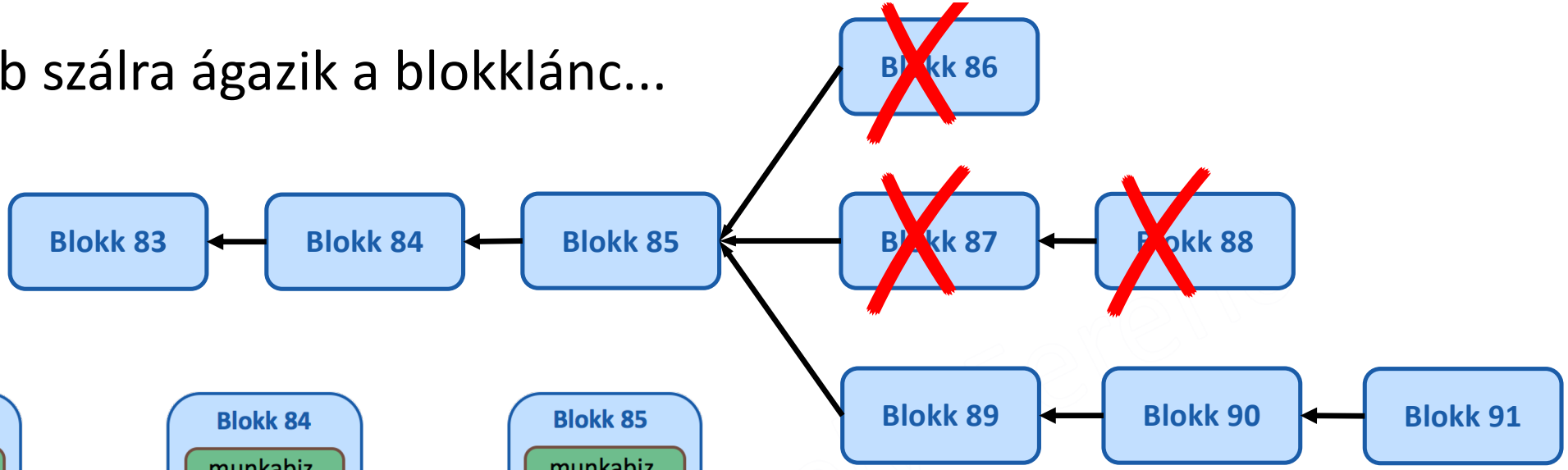
Minden blokk első tranzakciója a bányász jutalmát tartalmazza.

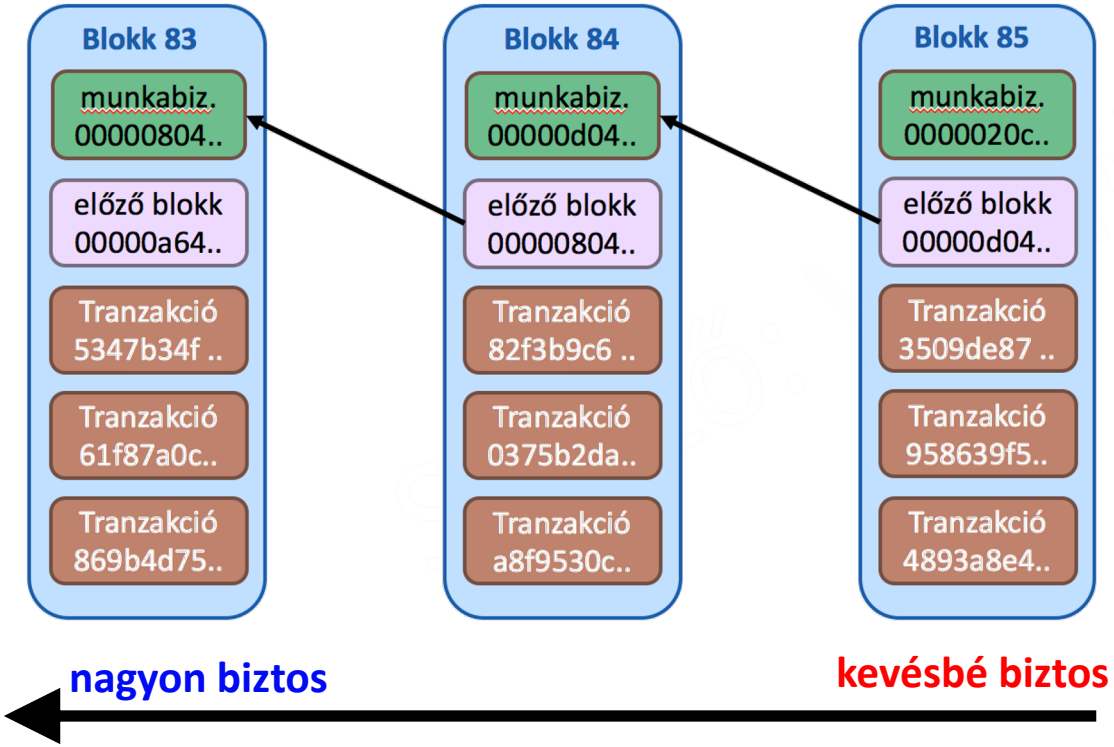


Blokkok és tranzakciók



Ha több szálra ágazik a blokklánc...

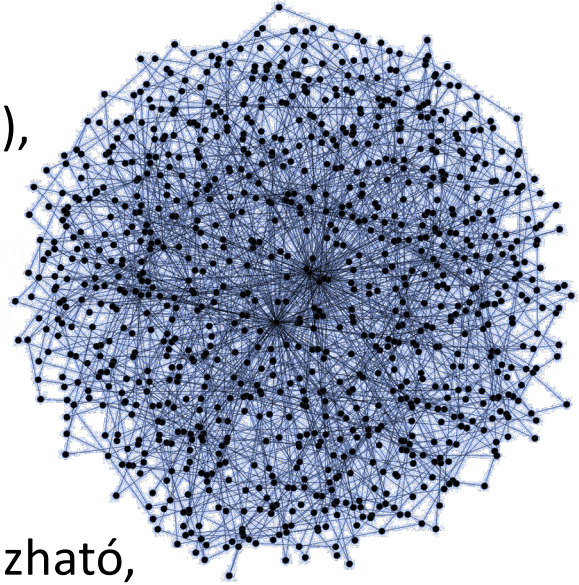




A mélyen beágyazott blokkok esetén egy visszamenőleges módosítási kísérlet után (pl. 83. blokkban) újra ki kell számolni a 84-es és 85-ös blokkok munkabizonyítékát, majd túl kell szárnyalni a teljes hálózat hash-számító képességét, hogy a közben elkészült blokkokat is újra számoljuk.

Az eredmény sokkal több, mint a cél (kriptopénz): hiteles adatkezelés

Elosztott adattároló rendszer, mely:



- ✓ tisztán a használók közötti kapcsolaton alapul (purely peer-to-peer),
- ✓ a rendszer teljesen decentralizált (mindenki egyenrangú),
- ✓ mindenki csak a saját adatairól (pl. pénzéről) rendelkezhet,
- ✓ visszamenőleg nem lehet adatot (tranzakciót) módosítani,
- ✓ az új adat (pl. pénz) létrehozási jogára szigorú szabályok hozhatók,
- ✓ a rendszer működtetésébe befektetett munka igazságosan jutalmazható,
- ✓ a résztvevők közötti eltérő adatok esetén a protokollt betartók gyorsan konszenzusra jutnak az érvényes adattartalmat illetően,
- ✓ a protokoll a kötelező, a szoftver nem (a blockchain maga a protokoll, a szoftverek csak megvalósítják) => nem kell másban (fejlesztőben) megbízni, a protokoll pedig nyilvános.