



és ami mögötte van

21 BTC
(total)

Csirmaz László, CEU

Bob



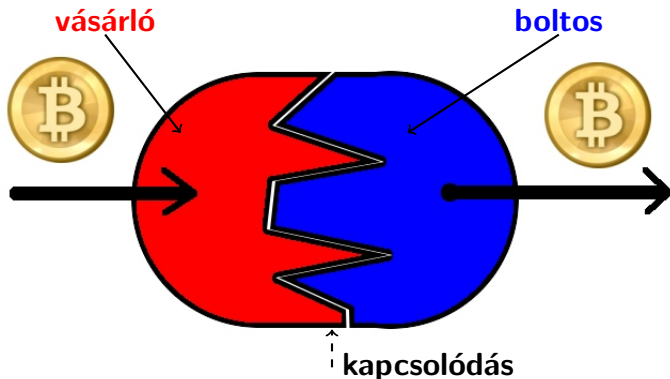
... wallet
... private
... keys (A,C,D)

Bob's wallet
has 2 private
keys (B,E)

Tartalom

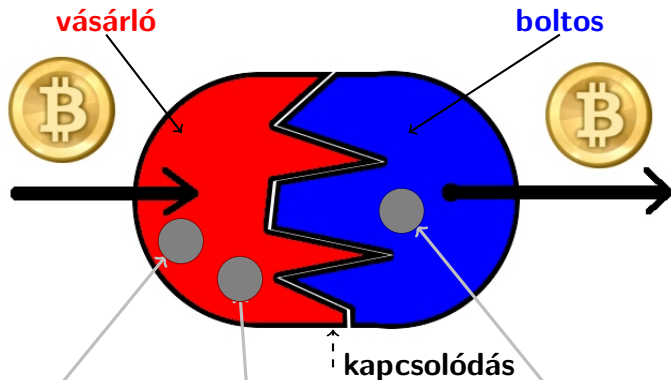
- 1 Bitcoin alapfogalmak
- 2 Bitcoin a felhasználó szemével (rövid)
- 3 Biztonság, kényelem, fenntarthatóság

Egy elektronikus tranzakció – amúgy általában



A **kapcsolódás** helyes, ha a tranzakció feltételei teljesülnek.
Elektronikus pénznél persze elektronikus(an kódolt) feltételek, pl:

Egy elektronikus tranzakció – amúgy általában

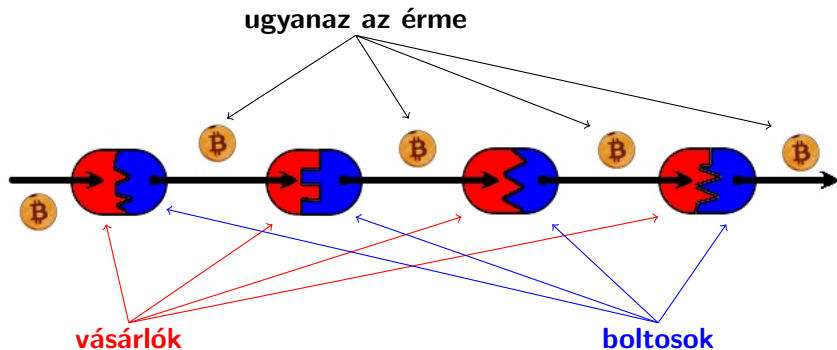


A **kapcsolódás** helyes, ha a tranzakció feltételei teljesülnek.
Elektronikus pénznél persze elektronikus(an kódolt) feltételek, pl:

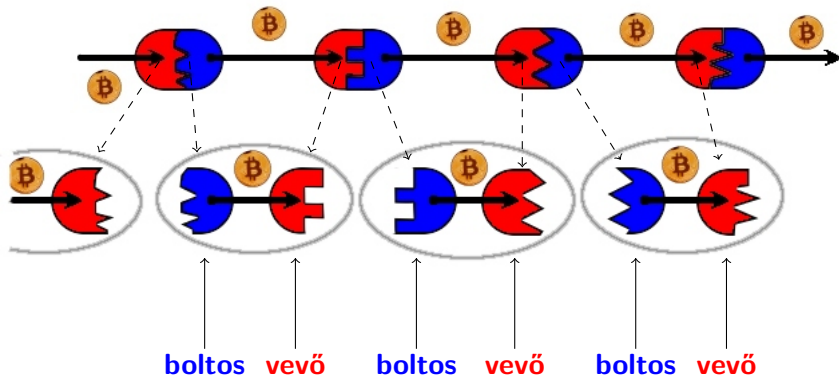
Ezzel a nyilvános kulccsal ezt írd alá.

Itt a kért aláírás.

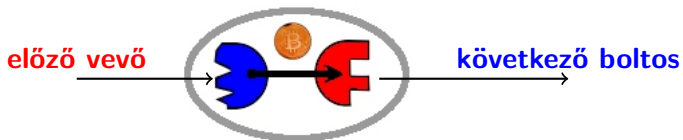
Elektronikus érme életútja



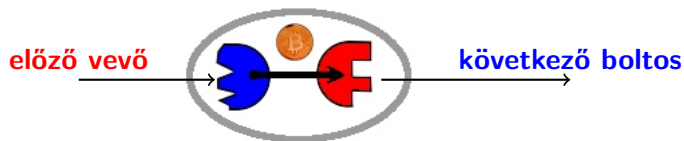
Hogy látja ezt a bitcoin?



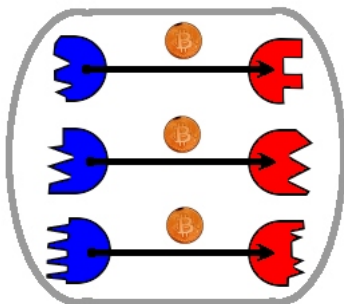
Egy bitcoin tranzakció



Egy bitcoin tranzakció

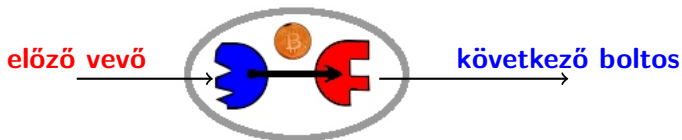


vagy inkább (gazdaságosabb):

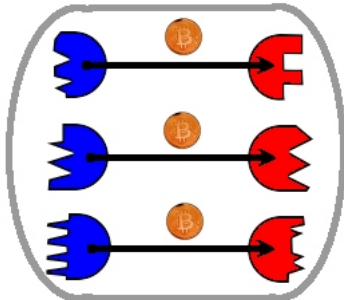


Az érmét nem lehet bontani!

Egy bitcoin tranzakció



vagy inkább (gazdaságosabb):

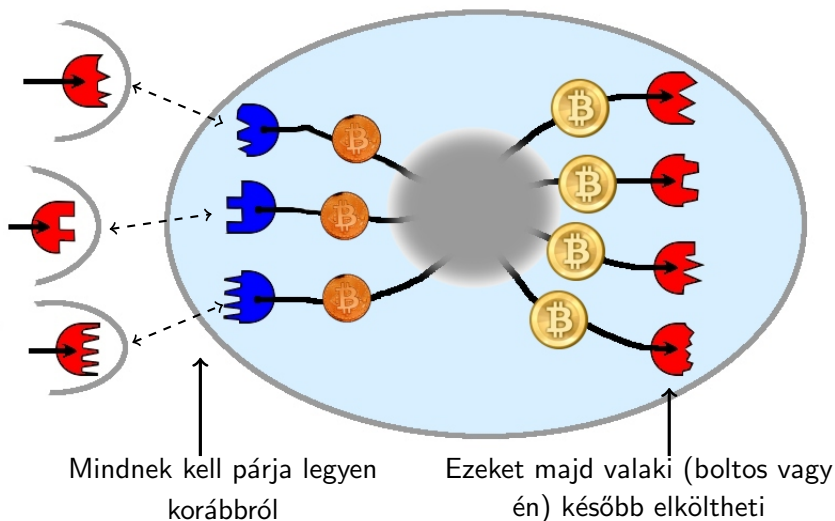


Az érmét nem lehet bontani!

Hogyan kapjuk meg
a visszajáró aprót?

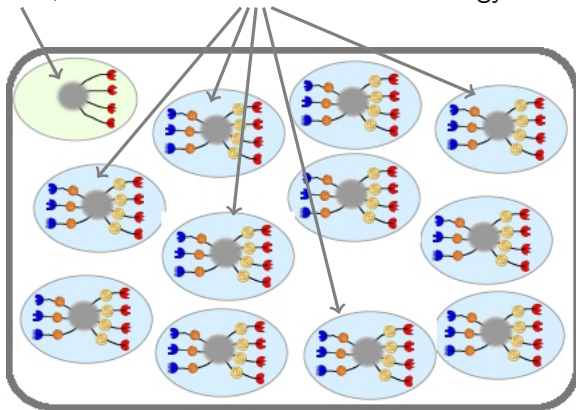


Sztenderd bitcoin tranzakció, amit a vevő állít össze



A bitcoin tranzakciós blokk – a bányászok készítik

Egy coin-base, és sok-sok *sztemderd* tranzakció egy blokkban:



Egy-egy új tranzakciós blokk átlag 10 percenként jelenik meg.

Bitcoin blokklánc – az összes eddigi bitcoin tranzakció

A blokklánc

- abszolút nyilvános, P2P hálózaton terjesztik
- lekérdezhető: <https://blockchain.info>
- a **bitcoin bányászok** tartják karban – bárki lehet bitcoin bányász, de a bekerülési költség ma már nagyon nagy
- jelenleg 44G; mérete a tranzakciók számával arányosan nő; tavaly több mint +20G
- P2P hálózat (mint bittorrent, skype), nincs központi szerv
- **minden** tranzakció nyilvános és vizsgálható, visszakereshető (de hogy ki és honnan töltötte fel a tranzakciót, az nem).

A bitcoin protokoll és azt megvalósító algoritmusok

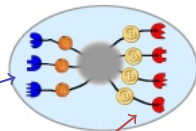
- abszolút nyilvános és ingyenes
- nincs mögötte semmilyen szervezet (és pl. garancia hogy nem változik)

Tartalom

- 1 Bitcoin alapfogalmak
- 2 Bitcoin a felhasználó szemével (rövid)
- 3 Biztonság, kényelem, fenntarthatóság

Hogyan vásárolunk bitcoin-nal?

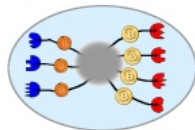
- A vevő összeállít egy tranzakciós blokkot



A bemenő fél tranzakciókat a vevő az érméihez tartozó titkos kulcsokkal érvényesíti;
a kimenőkbe a boltos által megadott nyilvános kulcsot írja,
a visszajáró részbe egy saját – új – nyilvános kulcsot ír.

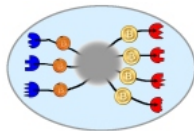
Hogyan vásárolunk bitcoin-nal?

- A vevő összeállít egy tranzakciós blokkot
- A vevő bedobja (feltölti) a “pool”-ba a blokkot, használva a bitcoin hálózatot.



Hogyan vásárolunk bitcoin-nal?

- A vevő összeállít egy tranzakciós blokkot



- A vevő bedobja (feltölti) a “pool”-ba a blokkot, használva a bitcoin hálózatot.

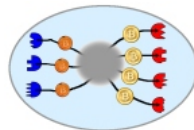


- A boltos megvárja, míg a tranzakció megjelenik a blokkláncban elég mélyen, hogy a blokk biztosan ne kerüljön visszavonásra (3–5 mélység elegendő, fél óra – több nap)



Hogyan vásárolunk bitcoin-nal?

- A vevő összeállít egy tranzakciós blokkot



- A vevő bedobja (feltölti) a “pool”-ba a blokkot, használva a bitcoin hálózatot.



- A boltos megvárja, míg a tranzakció megjelenik a blokkláncban



- Örülnek



Tartalom

- 1 Bitcoin alapfogalmak
- 2 Bitcoin a felhasználó szemével (rövid)
- 3 Biztonság, kényelem, fenntarthatóság

Előnyök és hátrányok

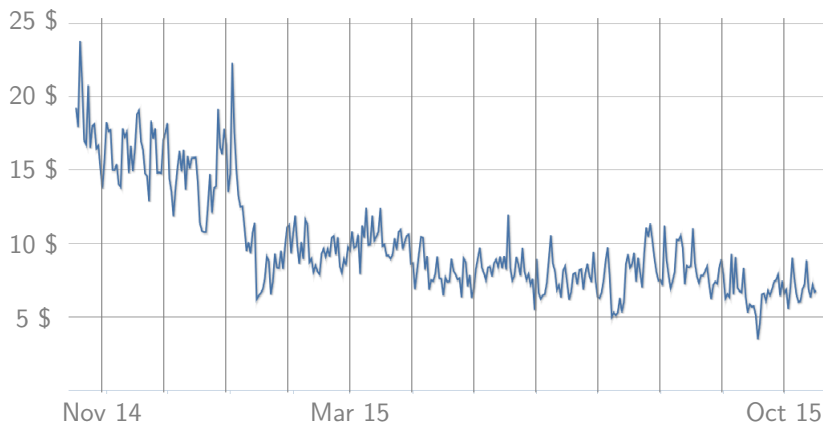
• PRO

- viszonylag kevés kripto technikát használ, de azt jól
- a sztenderd tranzakciók hibátlanok
- a fennállás óta (2009) nem volt sikeres kripto támadás
- terjed a használata

• KONTRA

- vannak nem sztenderd tranzakciók is (tipikusan elutasítják)
- a P2P pool-ba feltöltött tranzakciók integritása problémás
- egy rosszindulatú felhasználó tud “trükközni”
- tranzakciók visszavonása zavaros és esetleges
- kapcsolódó kényelmi szoftverek (wallet) gyakran hibásak
- a bitcoin elveszthető, ellopható, nem reklamálható
- nincs mögötte semmilyen “megfogható” garancia

Egy bitcoin tranzakció költsége



Ebből a tranzakció által fedezett rész csak **1%**, vagyis 6 cent.
A többit a rendszer termeli ki: ennyi “jutalom” jár a bányászoknak.

Megmarad? Fennmarad?

- Hosszú távú jövő: teljes bizonytalanság.
- A bitcoin elindítója szerint: társadalmi kísérlet.
- Előre megtervezett jövő, fix mennyiségű bitcoin létezhet.
- Lehetőségek:
 - két évenként duplájára értékelődik fel követve a még kibocsátható bitcoin mennyiséget
 - elértéktelenedik, nem éri meg dolgozni vele többé
 - megváltoztatják az előre fixált protokollt
 - megmarad egzotikus fizetőeszköznek
- Nem alkalmas nagy volumenű tranzakciók kezelésére – egyszerűen a blokklánc nem bírja követni.
- A múlt a kimúlásig kísérti: semmit nem felejteth!



Köszönöm a lehetőséget