Bitcoin vnitřnosti

Karel Bílek

Friday, January 31, 2014

Začneme od konce

- Co je cílem bitcoinu?
  - způsob, jakým poslat hodnotu online
  - decentralizovaně
- Všechno ostatní jsou jenom prostředky :)

Potřebuji zařídit jedinou věc...

- Jsem příjemce obnosu,
  - potřebuji vědět, že odesílatel skutečně obnos měl.

- ...to je v podstatě všechno.

Postavme si vlastní Coin!

Začneme jednoduše....

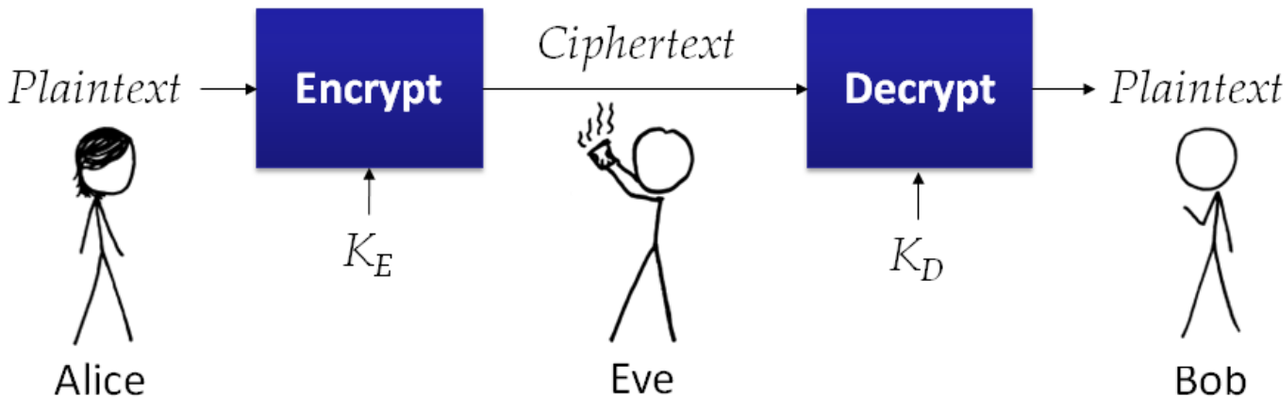
- Jde posílat jenom 1 Coin, jiná hodnota není možná
- Poslání proběhne tak, že já napíšu příjemci mail ve znění “Posílám ti 1 coin”

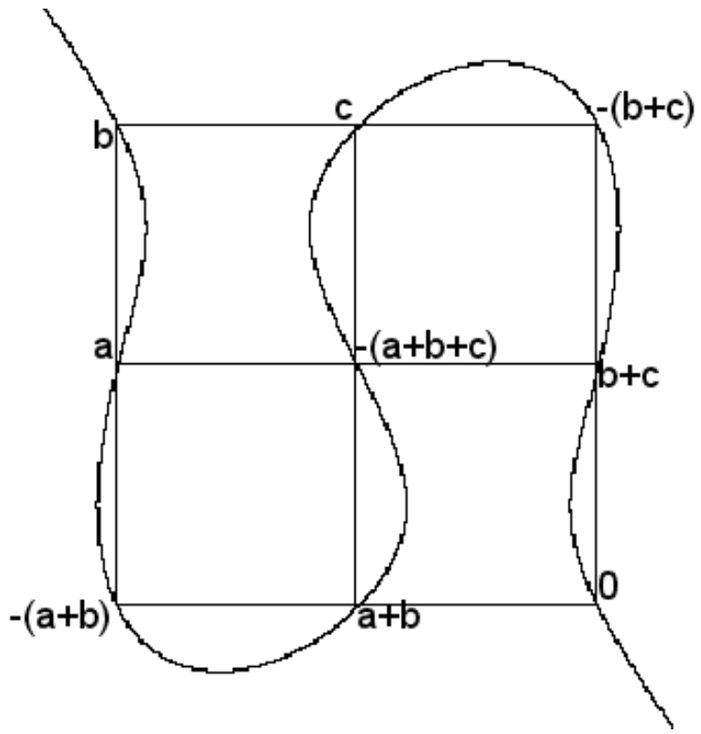
- Je to sice decentralizované, ale...
- odeslal to opravdu odesílatel?

Public/private key

- Jeden klíč k odemčení
- Jiný k zamčení
  - EC - elliptic curves
    - jeden z algoritmů
- operace s body na křivce

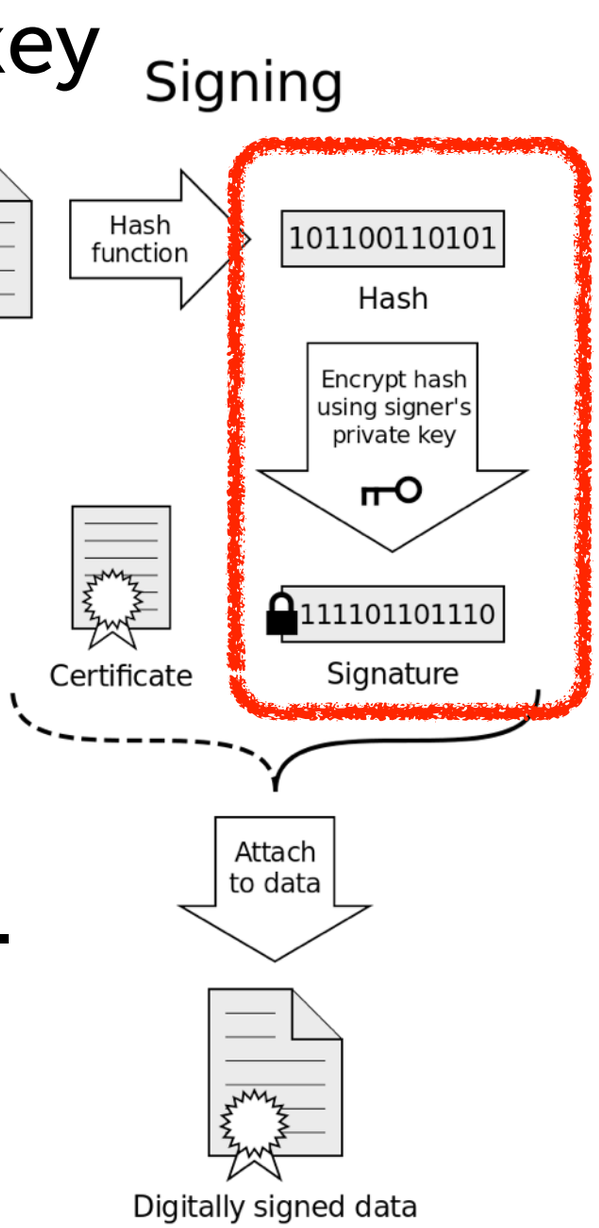
y^2=x^3+ax+b

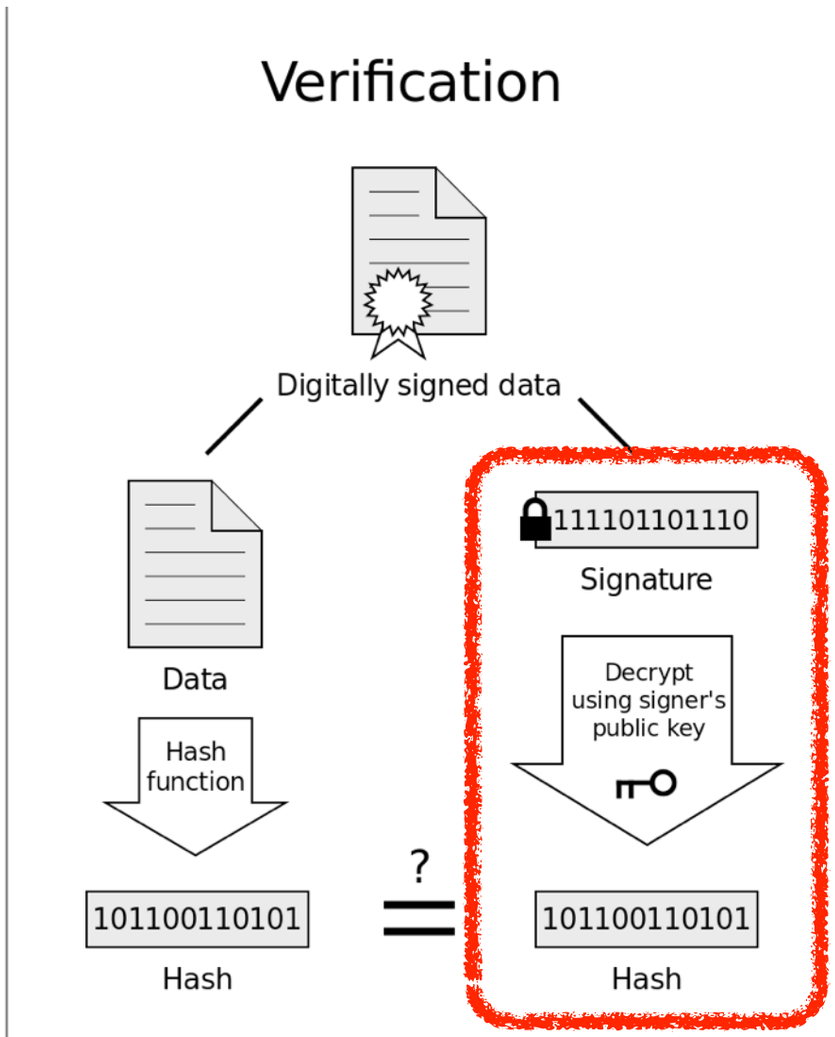




Podepisování přes asym. krypto

- Ověřovatel má public key a data
- ověří, že to skutečně odeslal odesílatel
- “drobnosti” jako hashing, padding apod.



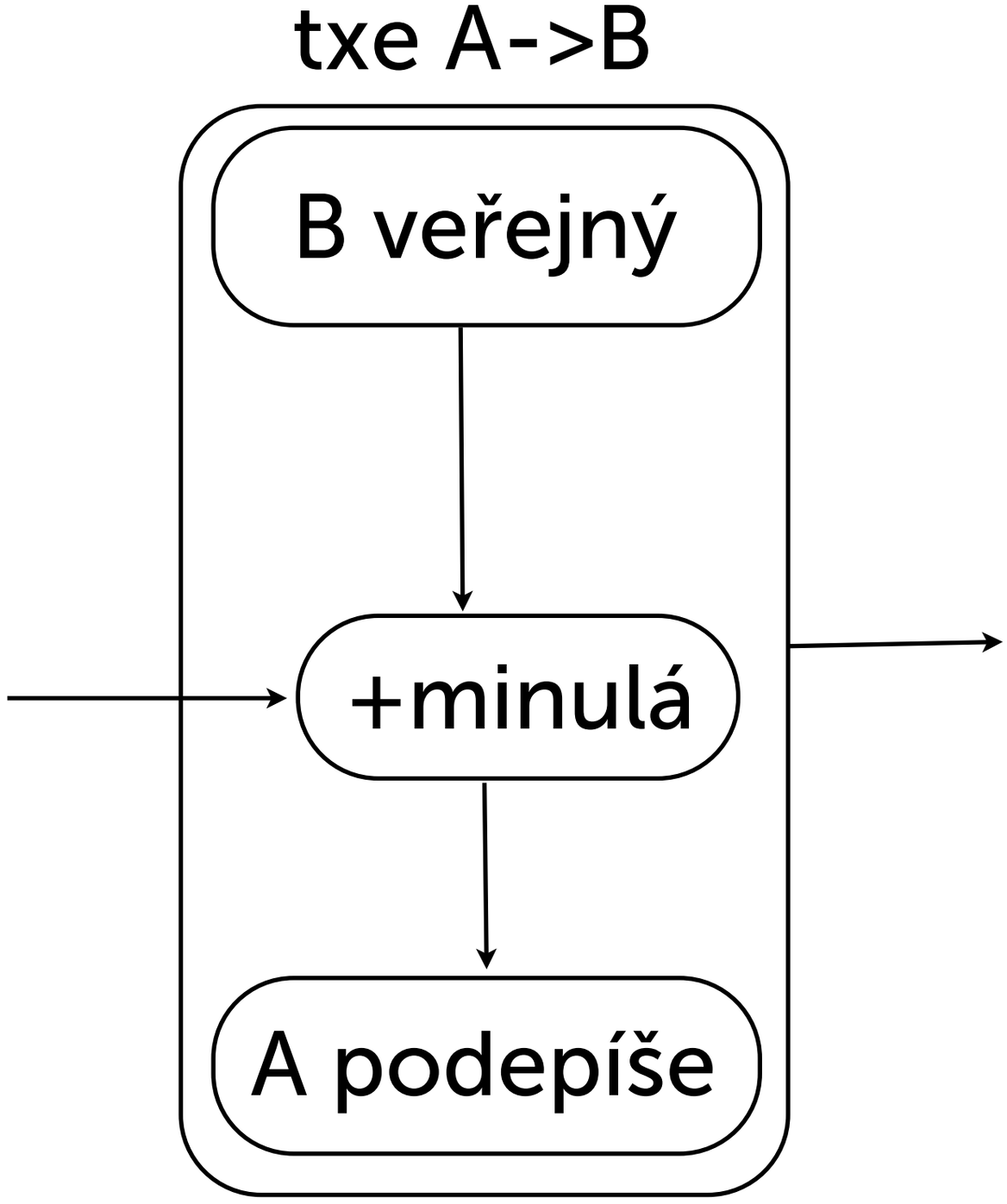


Trochu menší blbost

- Větu “odesílám 1 bitcoin” v mailu digitálně podepíšeme
  - sice je to autentifikované, ale nejde moc ověřit, že ten člověk

“Háčkujeme” transakce za sebe

- Existují “startovací” transakce, které jsou “platné”
- Spolu s vytvořením transakce pošleme historii



Vlastnosti našeho “systému”

- Funguje poměrně decentralizovaně :)
- můžu skutečně posílat jenom přijaté věci, ale!
  - musíme nějak vymyslet úvodní transakce
  - svůj Coin můžu poslat kolikrát chci - tzv. “double spend”

Řešení 1

- Přidáme centrálního kontrolóra
- Bude vydávat platné transakce a podepisovat je
- Všechny transakce půjdou přes něj
- Kontrolór platby zkontroluje, zveřejní a nějak podepíše

Vlastnosti našeho systému

- Moje peníze mi nikdo nevezme - kontrolór nezná můj privátní klíč
- Kontrolór může “maximálně” rušit transakce a nenechat mě peníze poslat.....
  - ....efektivně mě o peníze připraví
- Kontrolór může “zpětně” tvrdit, že nějaká transakce nebyla poslána

Řešení našeho problému....

- Kontrolóra decentralizujme!
    - pravé kouzlo bitcoinu :)
- ...a musím běžet na autobus :)