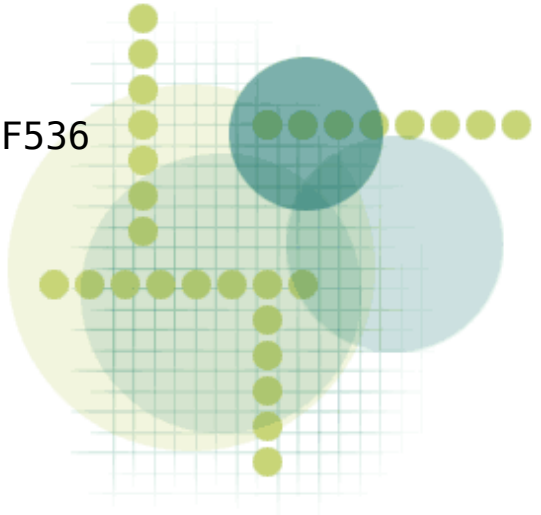
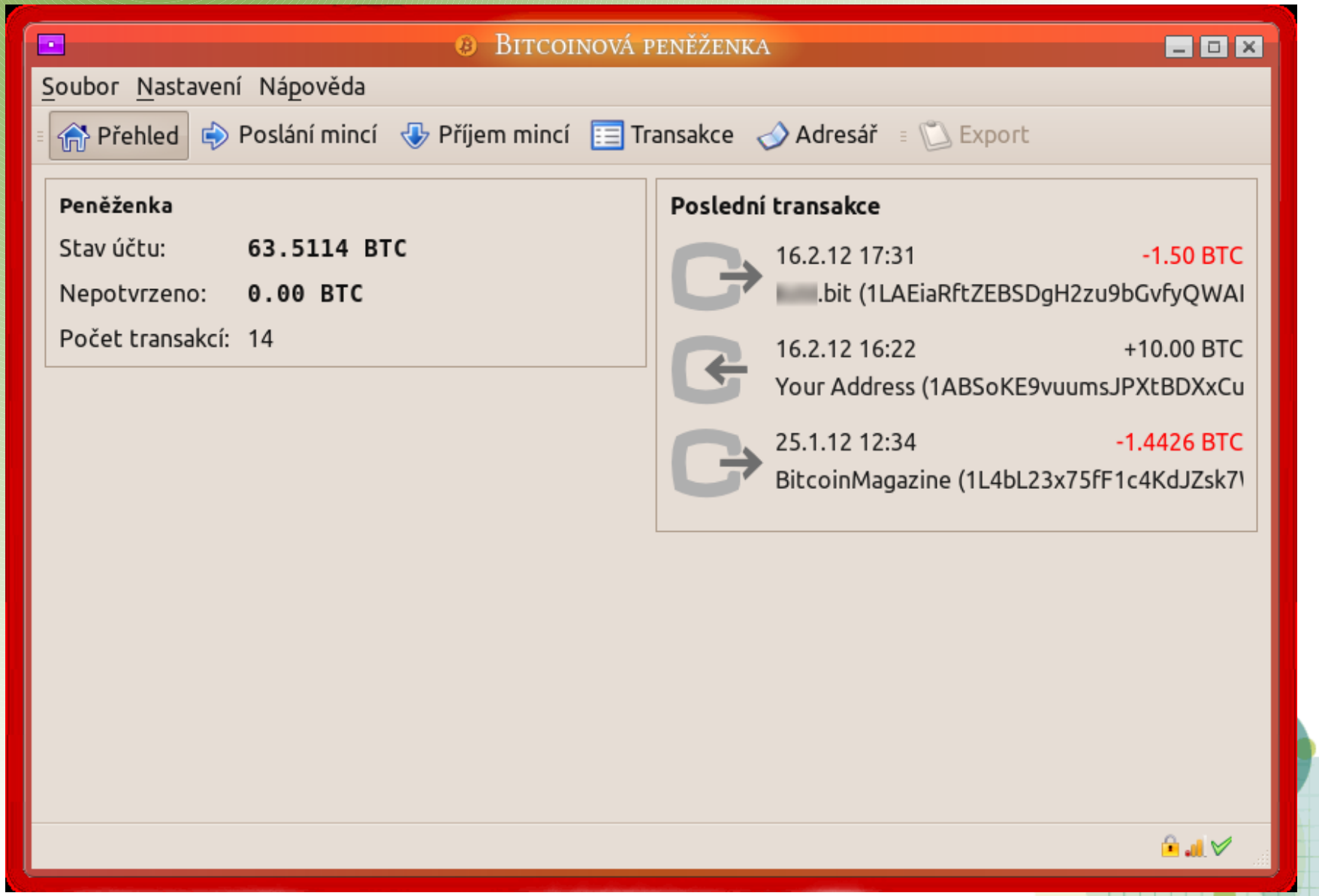
Bitcoin

jenda@hrach.eu

GPG 1D9D AC4B E964 0D1E 7F5D 6E03 B72F 6430 9FA4 F536




Bitcoinová peněženka
Soubor Nastavení Nápověda
Přehled
Poslání mincí
Příjem mincí
Transakce
Adresář
Export
Peněženka
Stav účtu: 63.5114 BTC
Nepotvrzeno: 0.00 BTC
Počet transakcí: 14
Poslední transakce
16.2.12 17:31 -1.50 BTC
.bit (1LAEiaRftZEBSDgH2zu9bGvfyQWAI
16.2.12 16:22 +10.00 BTC
Your Address (1ABSoKE9vuumsJPXtBDXxCu
25.1.12 12:34 -1.4426 BTC
BitcoinMagazine (1L4bL23x75fF1c4KdJZsk7

Bitcoin...

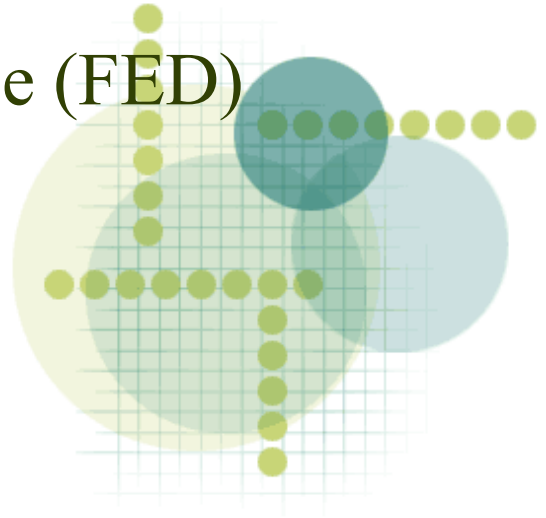
- je experiment v oblasti ekonomie, sociologie a kryptografie
- je decentralizovaný P2P měnový systém
- jsou peníze se skriptovacím engine

Co si ukážeme:

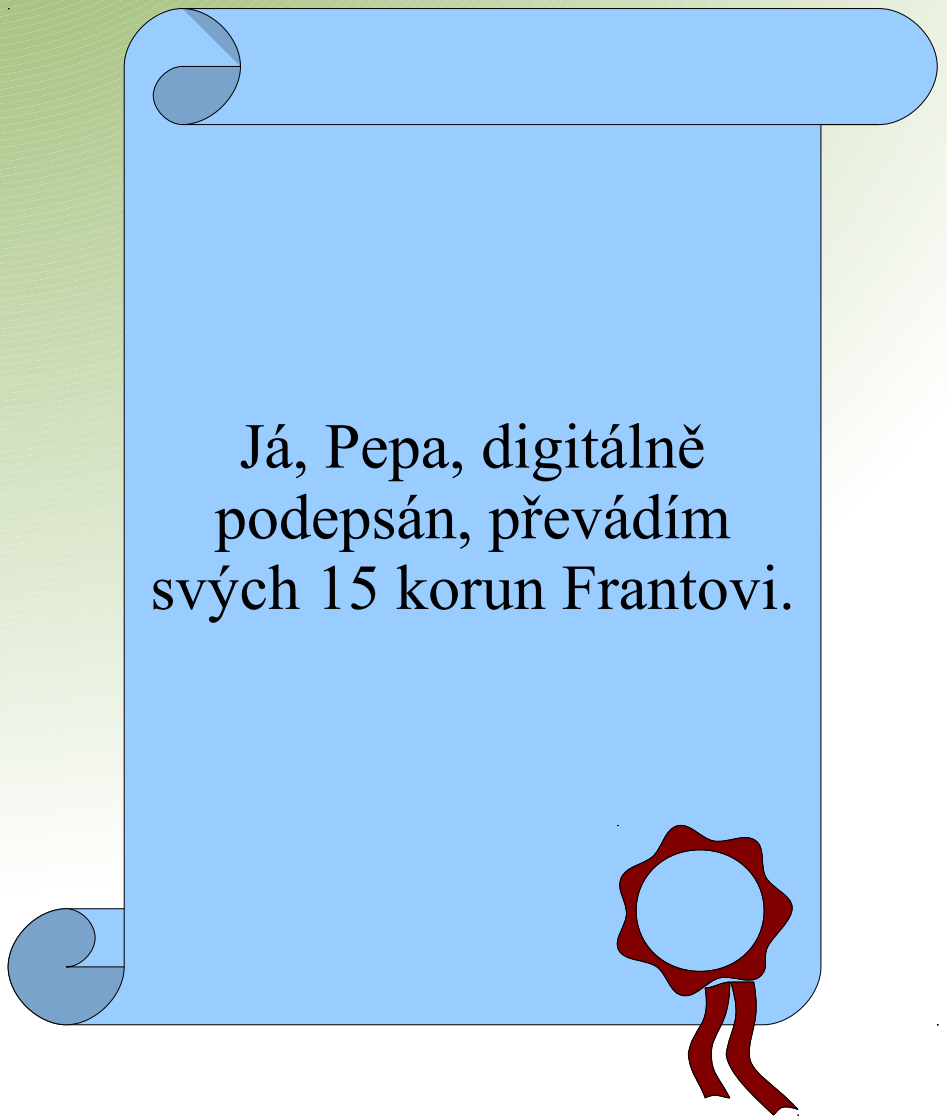
- Jak provozovat digitální měnový systém…
  - …bez centrální autority
- Jak udělat důvěryhodný timestamp
- Jak bezpečně platit na černém trhu (ehm)

Hotovost, kreditka?

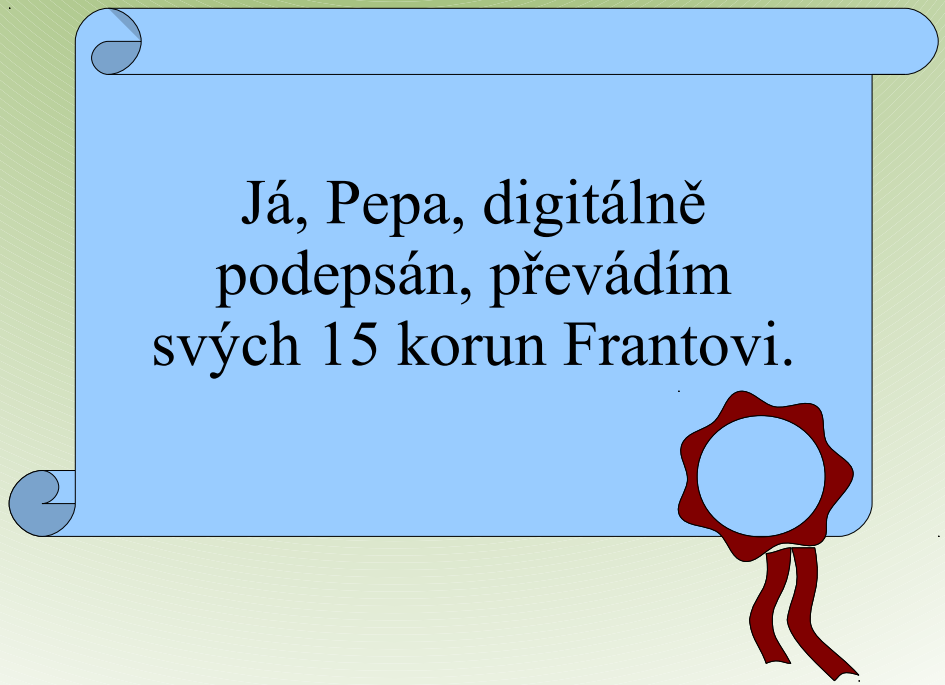
- Cash
  - celkem anonymní, nejde poslat po TCP/IP
- Kreditka, PayPal
  - neanonymní, zmrazení účtu (Wikileaks vs. Visa)
- Oboje fiat money
  - měnová reforma (ČSSR 1953), inflace (FED)

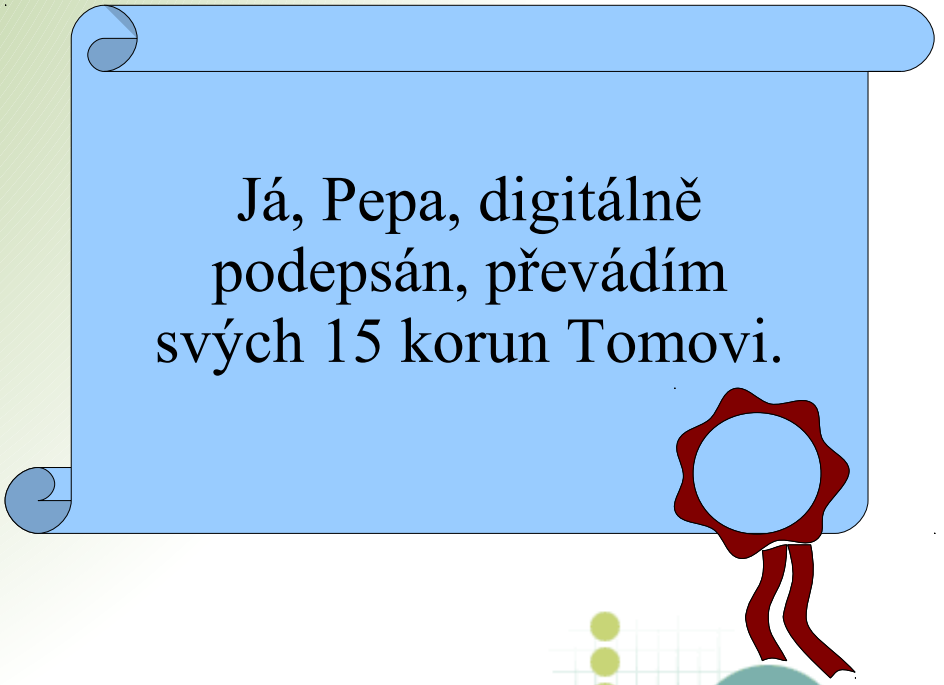


Digitální měnové systémy



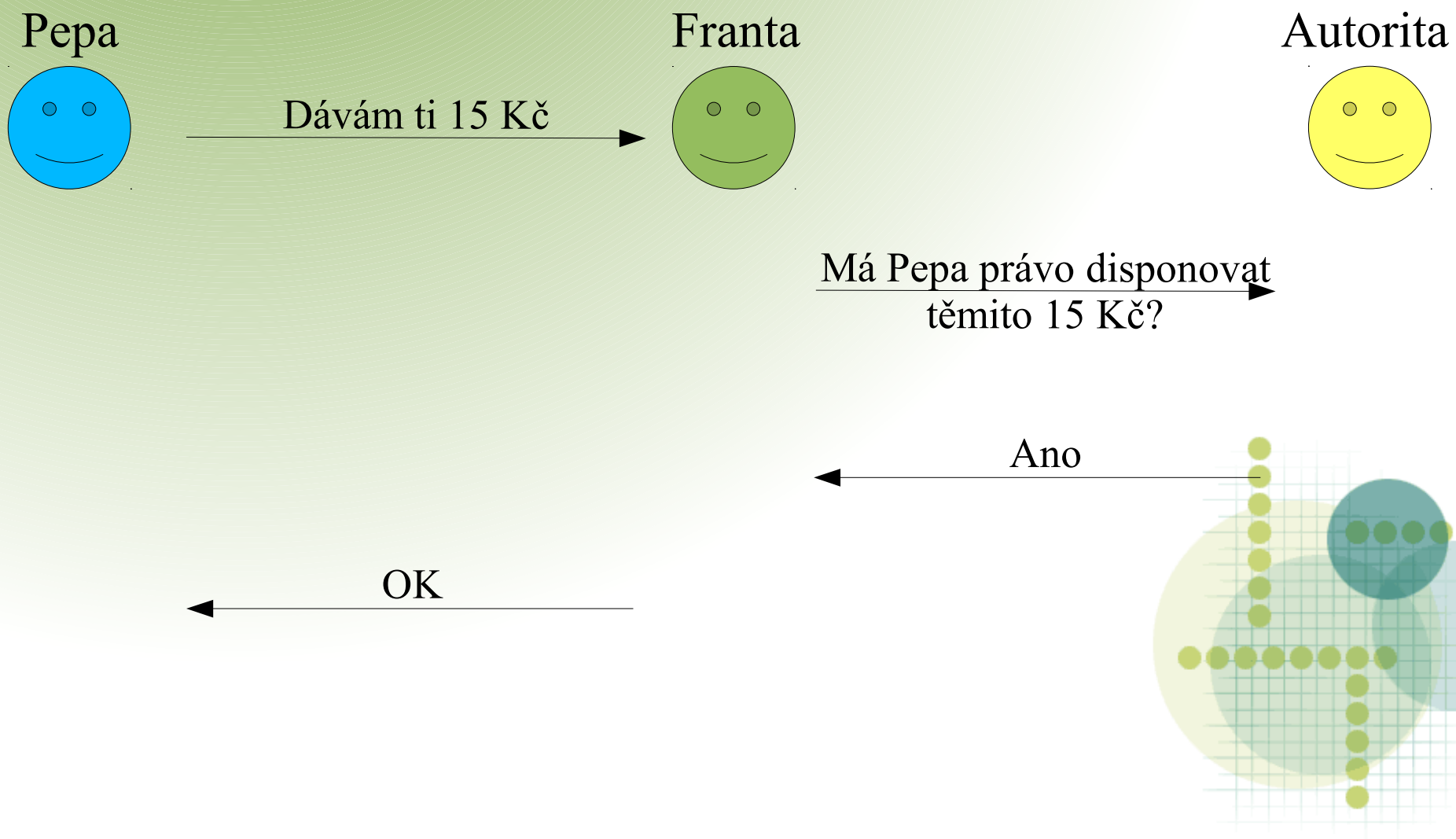
Double-spending





Franta musí být schopen ověřit, že peníze opravdu patří Pepovi.

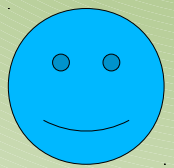
Řešení?


Pepa
Franta
Autorita
Dávám ti 15 Kč
Má Pepa právo disponovat těmito 15 Kč?
Ano
OK

Pepa

Franta

Autorita



Dávám ti 15 Kč

Má Pepa právo disponovat
těmito 15 Kč?

Ne

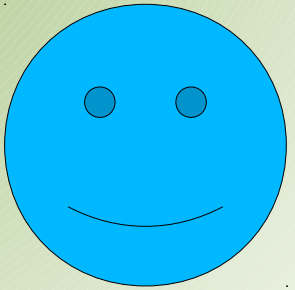
Podvodníku!

A dál?

Někdo musí vydávat peníze. Autorita?

radši ne…

Autorita = konsenzus



Hej vy všichni, má Franta tyto peníze?

Ano

Si piš

Jasně

Má

Co tvoří konsenzus?

- IP adresy?
  - 25.0.0.0/8 … UK Ministry of Defence
  - IPv6 /32 ≈ 79e+27
  - Tor není IP síť

???

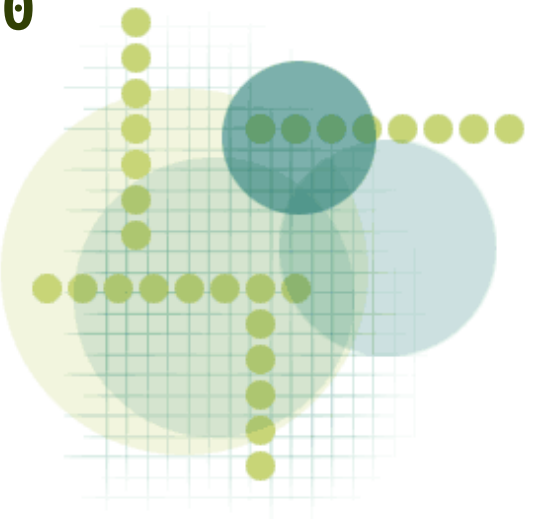
Výpočetní výkon!

Proof of work

- Řešíme složitý matematický problém
- Vyřešením jsme prokázali vlastnictví výpočetního výkonu
- Názor s největším prokázaným výkonem v síti „vyhraje“

Ukázka

- Chci, aby SHA256(“LinuxDays”+nonce) obsahoval na konci 2 nuly (**8** bitů nulových)
- Musím bruteforcovat…
  - `SHA256(LinuxDays0)   = …55ccd00b2`
  - `SHA256(LinuxDays1)   = …4bf5b8825`
  - `SHA256(LinuxDays290) = …dfcc6ca00`
  - `→ mám 8 jednotek výkonu`



A teď praktická realizace

- Na tabuli:
  - Chytání transakcí
  - Merkle tree
  - Blok
  - Blockchain

Tvorba Bitcoinů

- Coinbase „za odměnu“ v každém bloku
- V současnosti (10/2012) 50 BTC
- Brzy (12/2012) 25 BTC
- Celkem bude 21M BTC

Transakční poplatky

- Dobrovolné
- Ochrana proti DoS
- Motivace pro mining

Mining

- CPU (včera)
- GPU (dnes)
- ASIC (zítra)

- Pooled mining

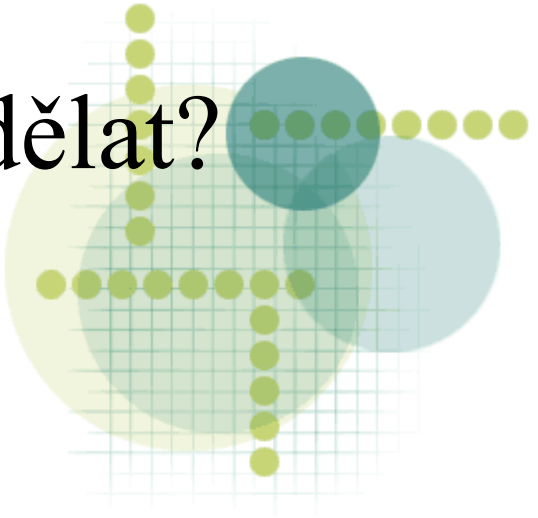
Útoky

- Ukradení peněženky
    - včetně poolů, směnáren…
    - nic s tím nejde dělat (not a bug)
- Double-Spend (nákladný)
- Botnet
- Cracknutí SHA256/ECDSA
- Cenzura (Tor)

Tolik k fungování systému.

(Dotazy?)

Část 2:
Co zajímavého se s tím dá dělat?



Volná diskuze...

- brmbar, SilkRoad
- směnárny, MtGox, Bitcoin-OTC, Localbitcoins
- Nákup v nedůvěryhodném prostředí
- Blockchain jako časová autorita (timestamping)
- Anonymní Bitcoin

Další čtení

- https://www.abclinuxu.cz/clanky/decentralizovana-kryptomena-bitcoin
- https://www.abclinuxu.cz/blog/jenda/2012/4/minimalisace-risik-potencialne-podvodnych-transakci
- http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization/