

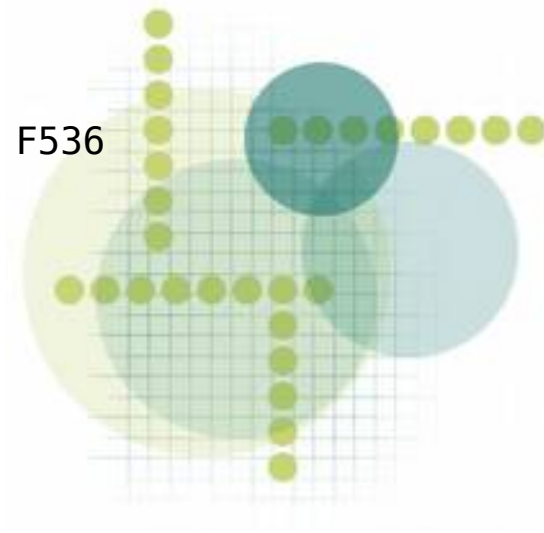
Bitcoin

Tato prezentace již ted':

<http://jenda.hrach.eu/f2/btc-cryptofest.pdf>

jenda@hrach.eu

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





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)
- A mnoho dalšího (s přesahem do diskuzní části po přednášce)

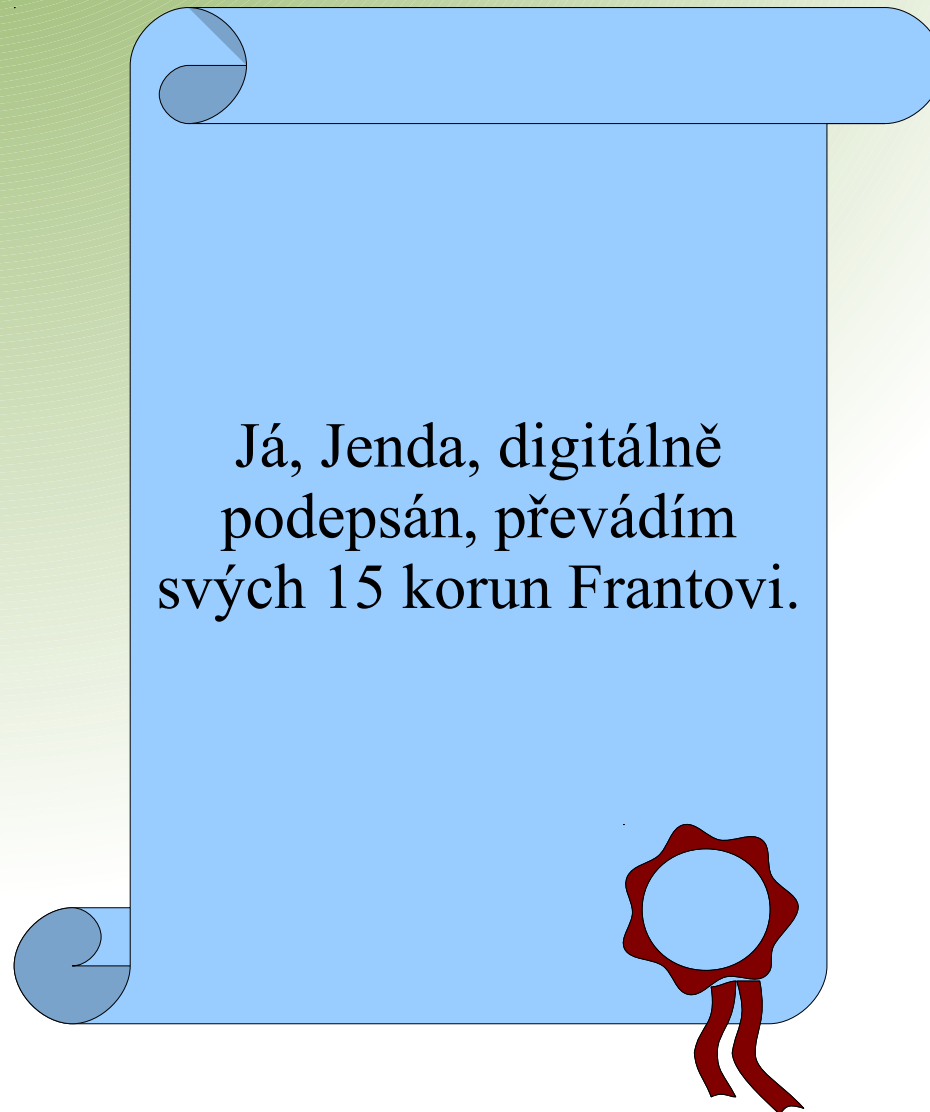


Hotovost, kreditka?

- 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)
 - Kypr (3/2013)



Digitální měnové systémy

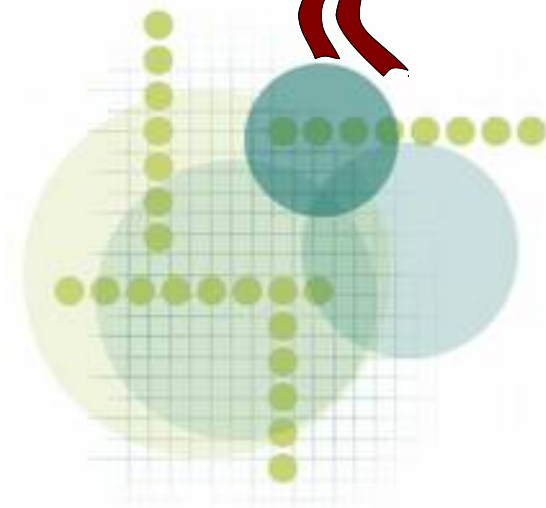


Double-spending

Já, Jenda, digitálně
podepsán, převádím
svých 15 korun Frantovi.

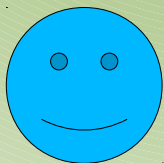
Já, Jenda, digitálně
podepsán, převádím
svých 15 korun Tomovi.

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



Řešení?

Jenda

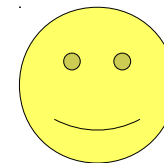


Dávám ti 15 Kč

Franta



Autorita



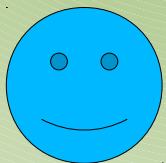
Má Jenda právo disponovat
těmito 15 Kč?

Ano

OK



Jenda



Dávám ti 15 Kč

Franta



Autorita



Má Jenda právo disponovat
těmito 15 Kč?



Ne

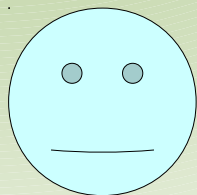
Podvodníku!

(zavření Liberty Reserve 5/2013)



A dál?

Někdo musí vydávat peníze. Autorita?



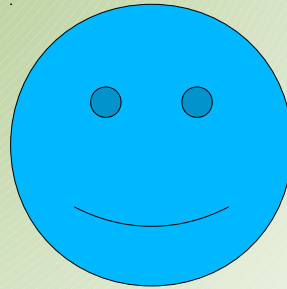
Vydej mi milion!!!



radši ne...



Autorita = konsenzus (P2P sítě)



**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 $\approx 79e+27$
 - Tor není IP síť

???

Výpočetní výkon!



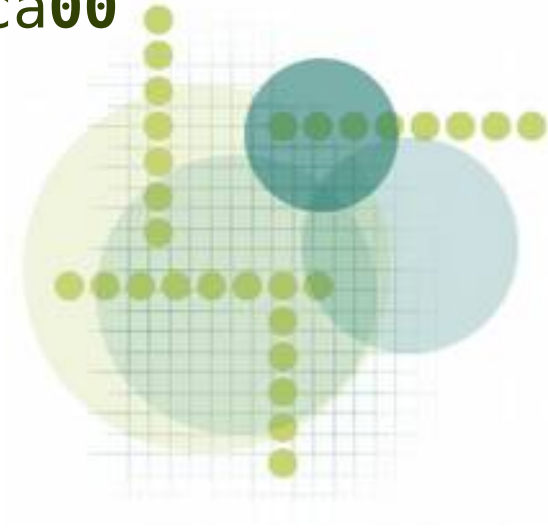
Proof of work

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



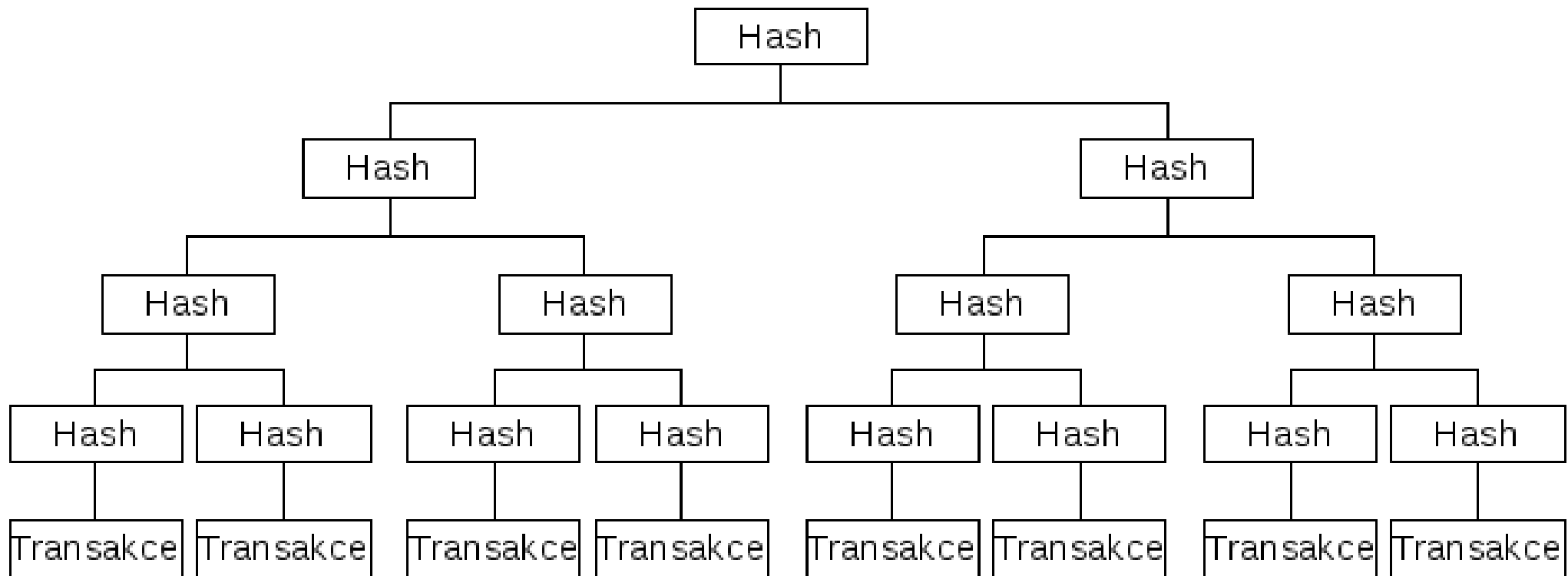
Ukázka

- Chci, aby SHA256(“LinuxDays”+nonce) obsahoval na konci 2 nuly (**8** bitů nulových)
- Musím bruteforcovat...
 - SHA256(LinuxDays0) = ...55ccd00b2
 - SHA256(LinuxDays1) = ...4bf5b8825
 - SHA256(LinuxDays290) = ...dfcc6ca**00**
 - → mám **8** jednotek výkonu



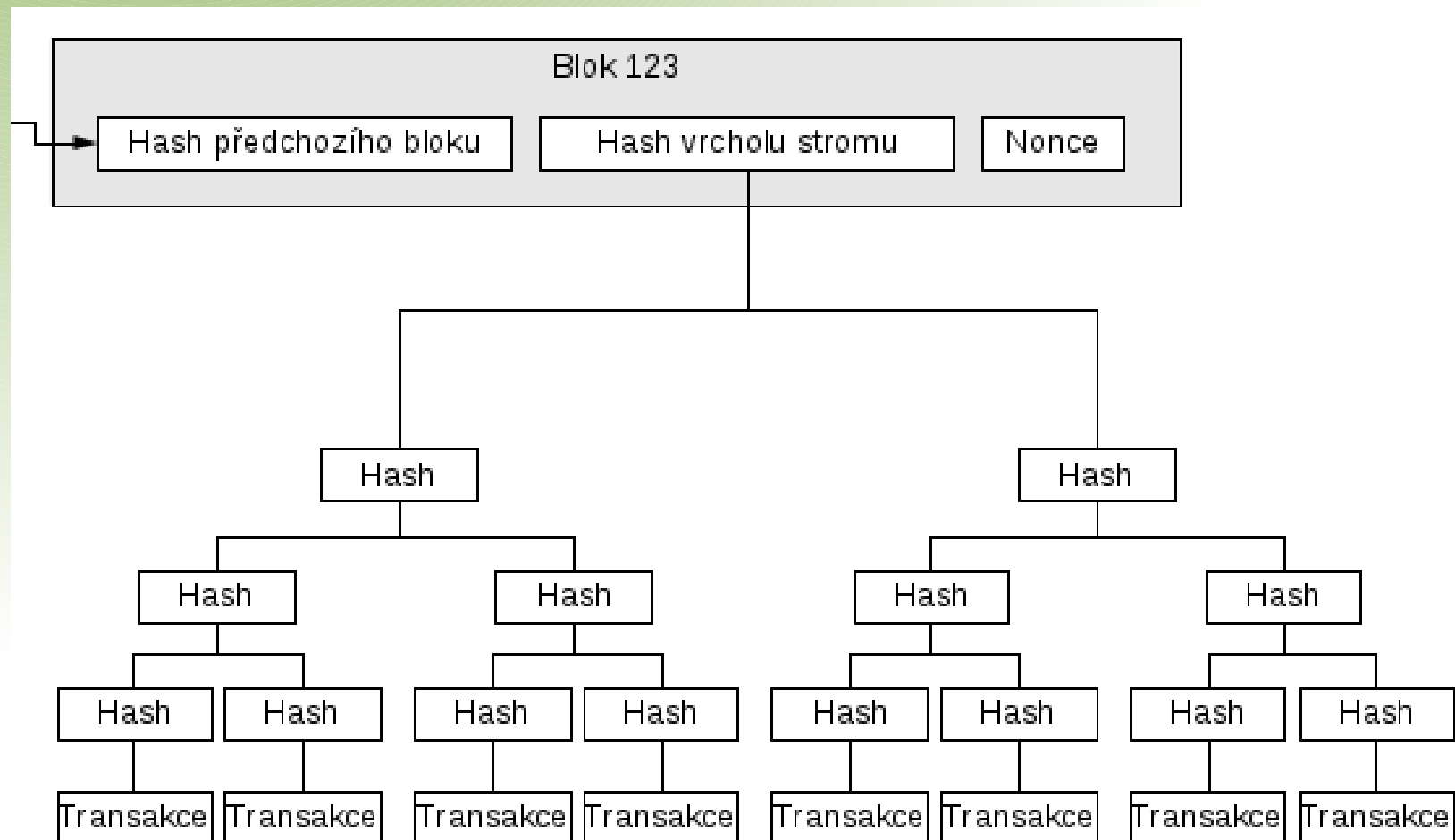
A teď praktická realizace

- Chytání transakcí, Merkle tree



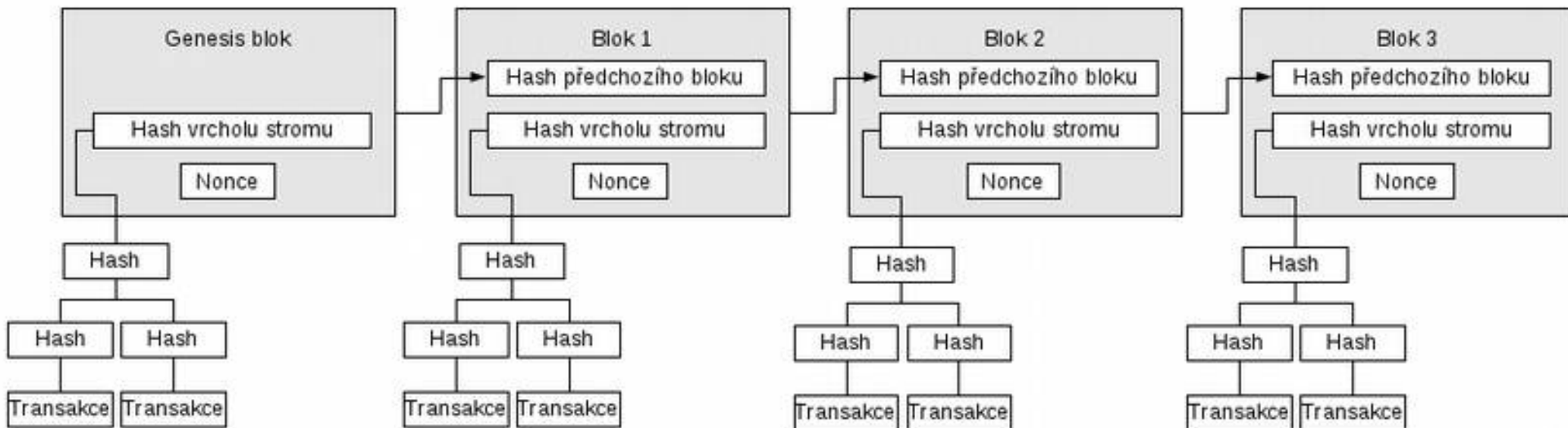
A teď praktická realizace

- Blok



A teď praktická realizace

- Blockchain

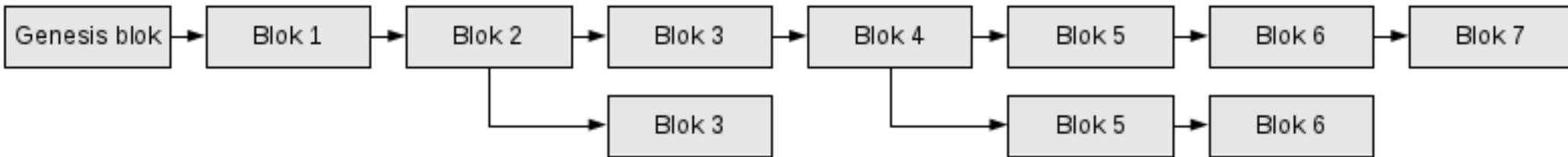


btw. timestamping, ukládání dat atd.



A teď praktická realizace

- Blockchain fork



- race condition, bug, útok na síť



Tvorba Bitcoinů

- Coinbase „za odměnu“ v každém bloku
- Postupně klesá
- V současnosti (2013) 25 BTC
- Celkem bude 21M BTC



Útoky

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



Konec?

- V diskuzní části se dozvíte:
 - jak je možné vlastnit půlku Bitcoinu
 - proč po vás klient chce transakční poplatek
 - jak se těžily Bitcoinu v minulosti a jak dnes
 - jak bezpečně obchodovat na černém trhu
 - proč nepoužívat oficiálního klienta
 - kde se za Bitcoinu můžete najít
 - ...a mnoho dalšího

Přijďte si popovídat nejen o Bitcoinu – na seminář nebo i jen tak

https://www.brmlab.cz/event/bitcoin_seminar

Dotazy?



Další čtení

Tyto slidy: <http://jenda.hrach.eu/f2/btc-cryptofest.pdf>

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



follow the white rabbit



Silk Road

anonymous market

messages 0 | orders | account

 a few words from
the Dread Pirate Roberts


Search

Go

logout



Shop by Category

Drugs 11,712

Cannabis 2,579

Dissociatives 215

Ecstasy 1,148

Opioids 611

Other 559

Precursors 105

Prescription 2,964

Psychedelics 1,425

Stimulants 1,553

Apparel 375

Art 2

Biotic materials 3

Books 934

Collectibles 19

Computer equipment 69

Custom Orders 90

Digital goods 697

Drug paraphernalia 373

Electronics 128

Erotica 649

Fireworks 11

Food 10

Forgeries 133

Hardware 34

Herbs & Supplements 14

Home & Garden 11

Jewelry 104

Lab Supplies 50

Lotteries & games 56

Medical 12


 10g MDMA Crystal - White
Regent Tested
\$5.31

 80mg Oxycodone (OP80)
- \$50 Each
\$0.39

 50 Gram TrainWreck
\$4.07

 4g Moonrock Methylone
99.8% (Highest Purity!)
\$1.75

 ATIVAN----
LORAZEPAM 2 mg (300)
\$1.48

 Ritalin - 54mg Extended
Release x 1
\$0.12

 3.3g / 1oz FULL MELT
Bubble hash - FREE FAST
\$5.14

 Stanol (Body Research),
200 tabs x 5mg
\$0.43

 14 grams Crystal
Methamphetamine
\$6.50

News

- Who's your favorite?
- Acknowledging Heroes

Transakční poplatky

- Dobrovolné
- Ochrana proti DoS
- Motivace pro mining



Mining

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



Volná diskuze...

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

