Bitcoin

Co to je a k čemu je to dobré?

Jiří Keresteš

Brmlab

2.6.2011

Co je to Bitcoin?

- Digitální měna nezávislá na centrálním subjektu
- Založen na deflačním modelu
- Maximální počet bitcoinů v oběhu je 21 milionů
- Odměna za vyřešení bloku se každé 4 roky sníží na polovinu
- Transakce jsou relativně anonymní - uživatel je reprezentován řetězcem
  (např. 1Ndx4BtSwpyWpGHopQ5fhbB5CB7LYHJFFR)

Jak můžu bitcoiny získat?

- Platba za služby, zboží, ...
- Výměnou za jinou měnu (Mt. Gox, #bitcoin-otc, ...)
- Mining
  - počítat lze i na GPU
  - samostatně vs. mining pool

Průběh transakce

1. Adresa současného majitele A v bitcoinu se změní na cílovou adresu uživatele B
2. Bitcoin se podepíše soukromým klíčem uživatele A
3. Záznam o transakci se broadcastem pošle ostatním, kteří ověří platnost podpisu
4. Transakce je považována za potvrzenou, když je obsažena v nějakém bloku z nejdelšího řetězu
   (nejdelší řetěz == nejvíce výpočetního výkonu == důvěryhodný zdroj)

Co je to ten blok?

- Blok se vytváří miningem
- Miner vezme transakce, přidá je do bloku a začne ho řešit
- Za vyřešený blok dostane miner odměnu, v současnosti je to 50 BTC + poplatky ze všech transakcí z bloku (transaction fees)
- Řešení bloku = hledání takového SHA-1 hashe bloku, který je nižší než současný *target*
- Pravděpodobnost vyřešení bloku za jeden pokus je v současné době okolo $5 \cdot 10^{-14}$ %

Další informace

`http://bitcoin.org` - oficiální web projektu
`http://weusecoins.com` - další informace
`http://blockexplorer.com` - prohlížeč bloků, transakcí, ...
`http://en.bitcoin.it` - neoficiální wiki
`http://bitcoin.org/bitcoin.pdf` - původní whitepaper od Satoshi Nakamota
`http://bitcoincharts.com` - různé finanční a technické údaje o systému