BitTorrent

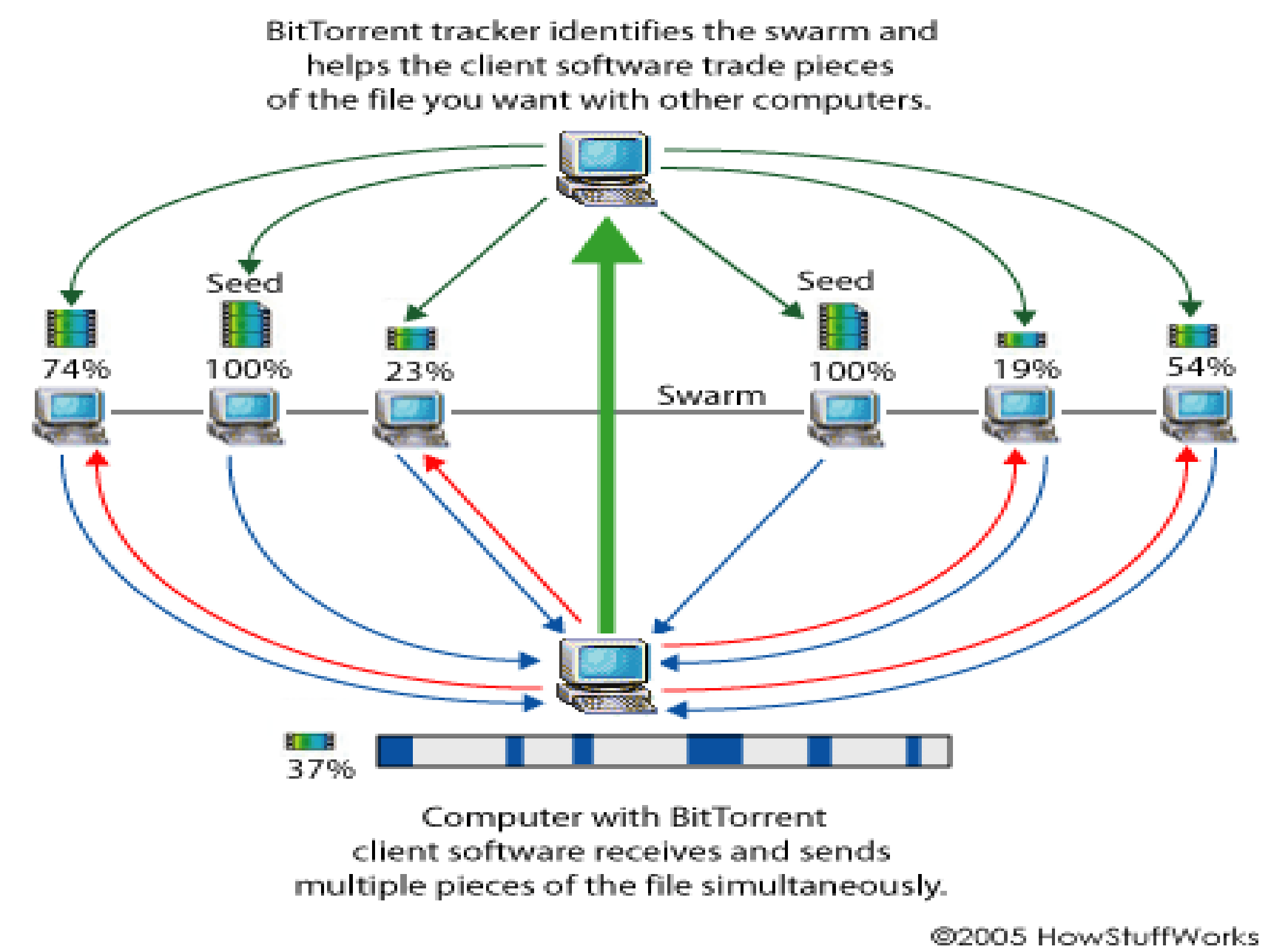
Vypracoval: Martin Fúsek
16.11.2007
X36MTI

Motivace

- Chci stahovat, nově vydaný soubor
- Poskytovatel nemá dostatek prostředku
  - Hardware (není až takový problém)
  - Bandwidth
- Použít bittorent, ušetření nákladů

Příklad: World of Warcraft

- 9.3 mil platicích užívatelů
- každé 3 měsíce patch, přidávající nový obsah:
  - 100MB až 2GB
  - průměrně 200MB
  - při 1GB = 10EB dat při dni, kdy se aplikuje patch
    - dokud se nestahne a nenainstaluje nejde hrát
    - doručení všem do 5h potřeba 5Tbit linky
    - TeliaSonera má pouze OC192 = 10Gbit
- => bittorent

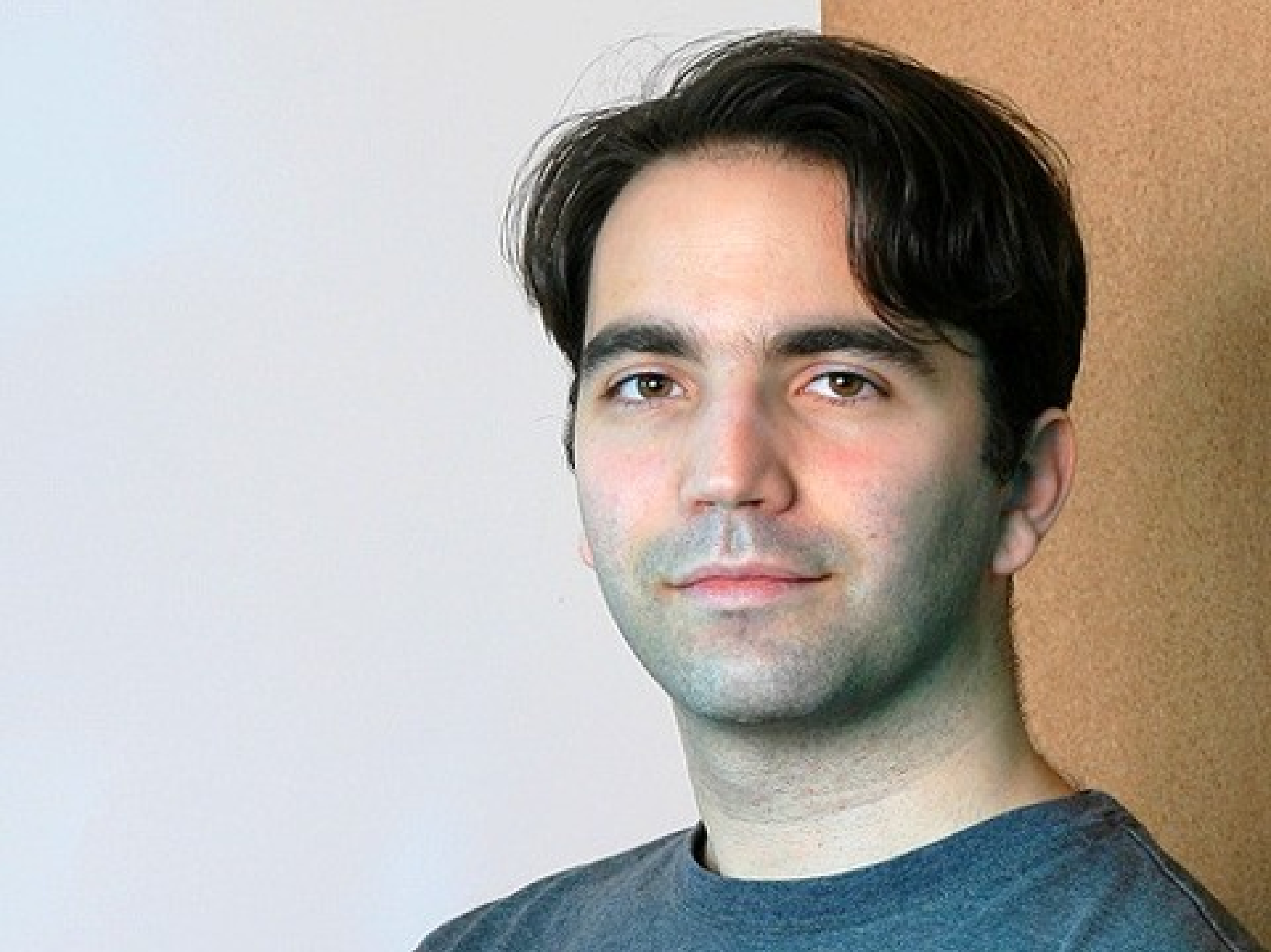

BitTorrent tracker identifies the swarm and helps the client software trade pieces of the file you want with other computers.
Seed
Seed
74%
100%
23%
100%
19%
54%
Swarm
37%
Computer with BitTorrent client software receives and sends multiple pieces of the file simultaneously.
©2005 HowStuffWorks

Nomenklatura

- Torrent
- Tracker
- Peer
- Seeder
- Leech
- Scrape
- Announce
- Swarm

Pachatelé

- Zakladatel: Mike Hawk (2001)
- Bram Cohen, CEO fy. BitTorrent, Inc.
  - Starší verze Open Source
  - Novější bude uzavřena



Bencoding

- **string**: <délka v ASCII>:<data>
- **Integer**: “i“<ASCII>“e“
- **lists**: “l“<bencoded values>“e“
  - *l4:spam4:eggse = ["spam", "eggs"]*
- **dictionaries**: d<bencoded string><bencoded element>e
  - *d3:cow3:moo4:spam4:eggse = { "cow" => "moo", "spam" => "eggs" }*

.torrent file

- Bencoding
  - info
    - piece length
    - pieces string složený z 20-byte SHA1 hash
    - private
    - .....
  - announce/announce-list
  - creation date
  - comment
  - created by

.torrent file II

- Jeden soubor na torrent
  - name
  - length
  - md5sum
- Více
  - name
  - files
    - length
    - md5sum
    - path

Komunikace tracker<->peer

- HTTP/HTTPS GET (RFC1738)
- Bencoding
- Response:
  - interval
  - complete
  - peers
    - peer id
    - Ip
    - port

Komunikace peer<->peer Handshake

- pstrlen délka pstr
- pstr identifikace protokolu „BitTorrent protocol“
- reserved
- info_hash hash SHA1 (jenom)info části .torrent souboru
- peer_id 20bajtů
  - „-“<2 písmena určující klienta><4 čísla pro verzi><random>

Komunikace peer<->peer Message

- <length prefix 4B BE><message ID><payload>
  - **keep-alive**: <len=0000>
  - **choke**: <len=0001><id=0>
  - **unchoke**: <len=0001><id=1>
  - **interested**: <len=0001><id=2>
  - **not interested**: <len=0001><id=3>
  - **bitfield**: <len=0001+X><id=5><bitfield>
    - které části mam, hned po handshake
  - **have**: <len=0005><id=4><piece index>
    - dodatečné oznámení vlastnictví po stahnutí

Komunikace peer<->peer Message II

- **request**: <len=0013><id=6><index><begin><length>
- **piece**: <len=0009+X><id=7><index><begin><block>
  - data
- **cancel**: <len=0013><id<=8><index><begin><length>
  - už ty data nechci
- **port**: <len=0003><id=9><listen-port>
  - port pro DHT

Algoritmy

- Downloading strategy
  - random
  - rarest first
  - pracuje se na streamování
- Super Seeding
- End Game
- Choking and Optimistic Unchoking
  - Tit for tat
- Anti-snubbing

Algoritmy II

- DHT
- Connection Encryption
  - PHE jen hlavičky, starší
  - MSE/PE
  - RC4
    - koresponduje 60–80bitum simetrické šifry
    - ale rychlé pro CPU

Implementace

- BitTorrent – python
- Azureus – Java
- µTorrent – C++
- Opera
- HW – některé routery

Nevýhody

- Snadno zjistitelný
  - poskytovatelem
  - RIAA atd... přes tracker
- Pomalý rozjezd
- ISP zakazují i pro legalní účely, 2x zatěžují FUP
- Přetěžuje směrovací tabulky
- Není řešeno vyhledávání
- Vymírání torrentů

Další doporučené počteníčko

- http://wiki.theory.org/BitTorrentSpecification