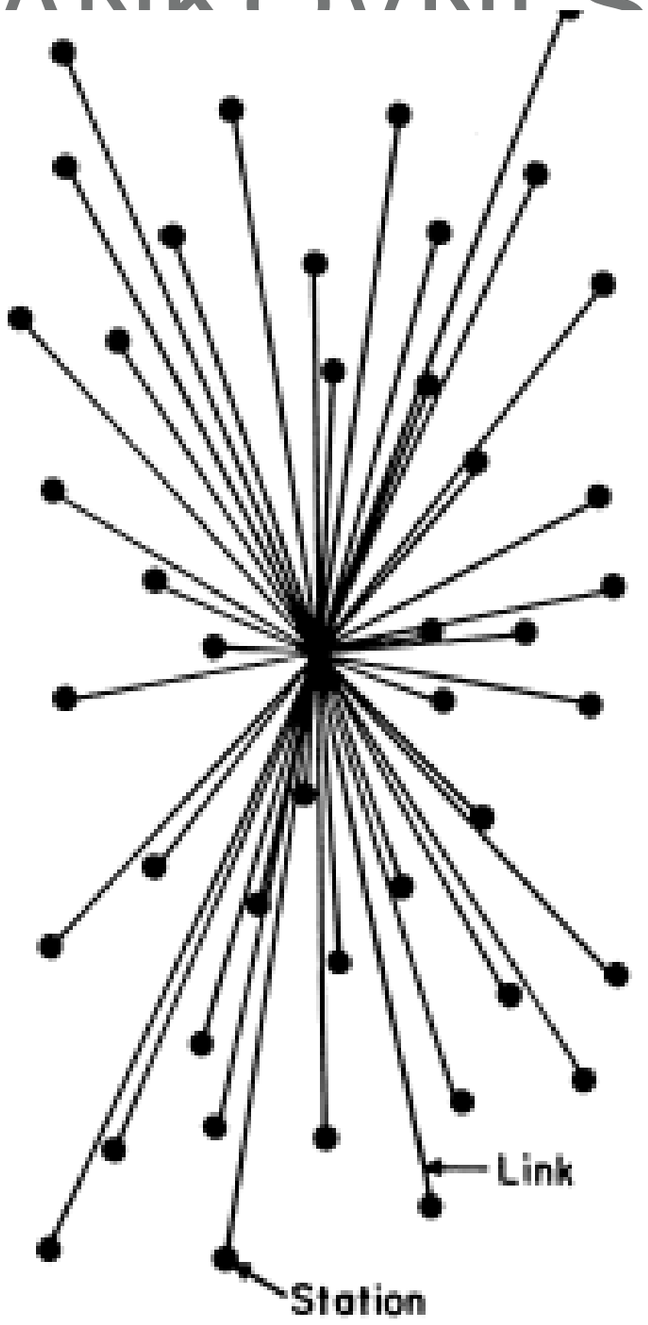
BLOCKCHAIN A BITCOIN

Jan Hanzelka

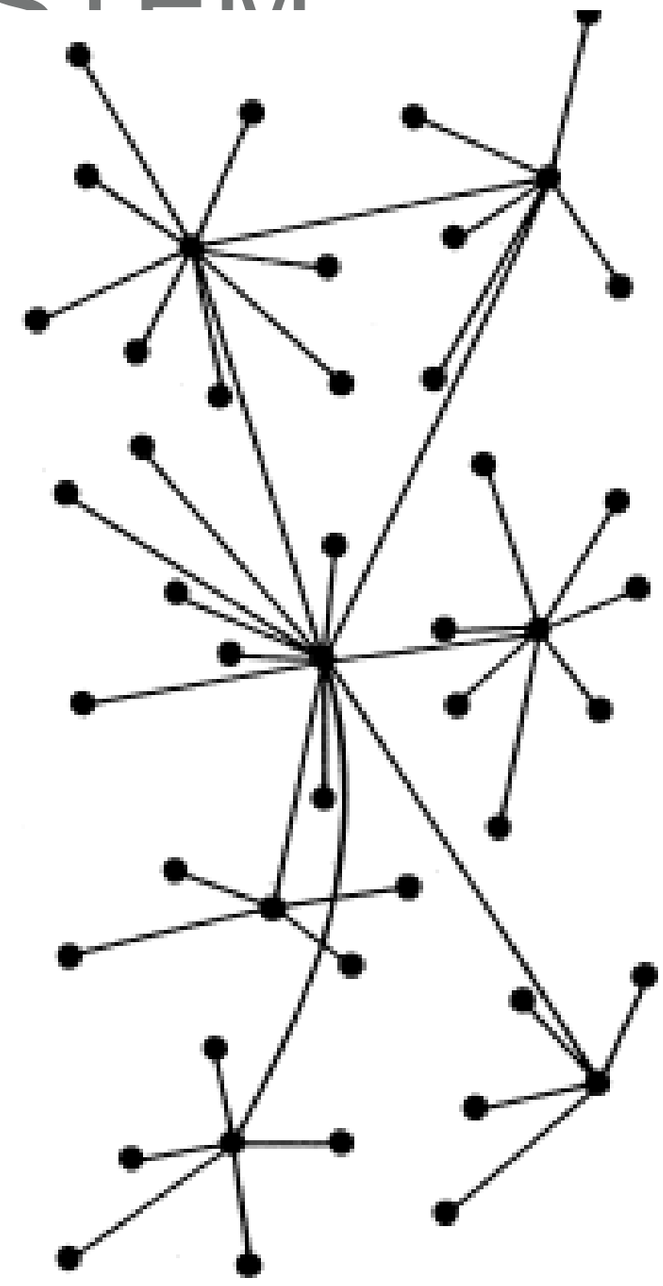
OBSAH

- Proč existuje bitcoin?
- Jak funguje blockchain?
- Jak funguje těžba bitcoinu?
- Jak nakoupit bitcoin?
- Jak jednoduše přijít o bitcoiny?
- Jaké jsou nejčastější podvody?
- Je bitcoin hrozba?

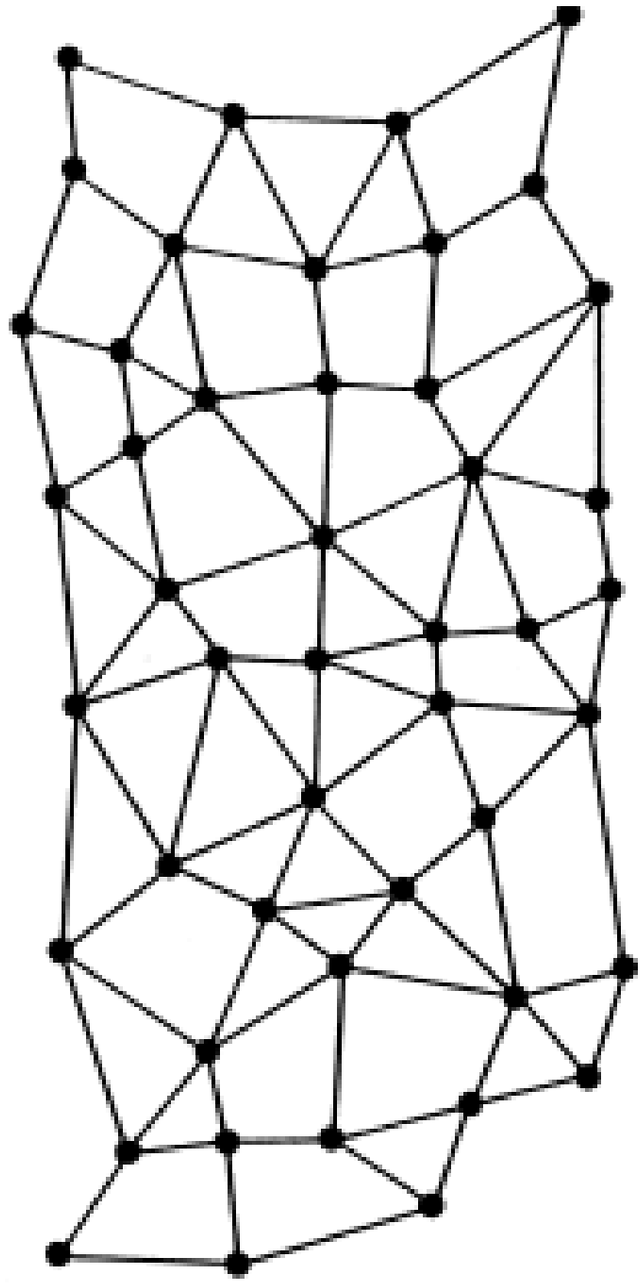
BLOCKCHAIN A DECENTRALIZOVANÝ BANKOVNÍ SYSTÉM



CENTRALIZED
(A)



DECENTRALIZED
(B)



DISTRIBUTED
(C)

BLOCKCHAIN JAKO UČETNÍ KNIHA

- cca 150 GB dat (Bitcoin)
- Chrnologicky řazená a neměná databáze
- Nezávislé auditovatelná
- Transakce tvoří bloky dat (určitý počet transakcí), na který navazují další bloky (cca1 MB co 10 min)
- Proof of Work -> nákladnost zápisu transakce
- Těžaři -> správci učetní knihy
  - odměňování (nové mince + transakční)
- Snaha prolamit učet vs. těžení

TRANSAKCE A JEJICH PROBLÉMY

Honza

Jakub

Vendula

- Autorizace
- Replay útok
- Double spending

TRANSAKCE JSOU NEMĚNÉ

- Zaslání na adresu s překlepem
- Zaslání špatné osobě
- Zaslání na adresu pro jinou měnu


EVGA GEFORCE GTX 1060

Honza

Jakub

Vendula

Mirka

Petr

Ondra

Miloš

ODKAZY

- http://yogh.io/#mine:last

BITCOIN

- začátek rok 2009
- Satoshi Nakamoto - White paper
- 0.00000001 BTC = Satoshi
- max 21 000 000 BTC
- vytěženo cca 17 mil BTC
- 12.5 nových bitcoinů cca každých 10 minut (2016–2020)

NÁKUP A PROVEDENÍ TRANSAKCE

- Směnárny
- Burzy
- Bitcoin ATM
- Osobní směna

MOŽNOSTI NEÚMYSLNÉ ZTRÁTY BITCOINU

- Chyba jednotlivce a rizika spojená s chybějícím garantem transakce (ztracení privátního klíče)
- Technické problémy (doba trvání transakce, poplatky)
- Krach burzy
- Možnosti nabourání se do účtu?

PODVODY

- "Prodám iPhone nevhodný dárek za 5000 Kč" jako číslo účtu uvedu účet směnárny a variabilní symbol svou BTC adresu
- "Rybaření"
- Praní výnosu z podvodu
- Nákup na falešné doklady
- Cryptolocker
- Replay útok skrze forknutou měnu
- Ponzi

OSTATNÍ KRIMINALITA

- Nákup léčiv - eshopy bez bankovního účtu
- gambling
- Možný nákup ostatních nelegalních služeb a zboží

Address for account **Bitcoin (legacy)**

12ctBkUVAnak9AGyRURkQY2mT2sBUtBd2L

Děkuji za pozornost

KONEC