FAKULTA
INFORMATIKY
Masarykova univerzita

# Od Ƀitcoinu ke kryptoměnám

Michal Zima

# Já a kryptoměny

- Bitcoin používám od začátku roku 2011.
- Se Slushem jsem zakládal IRC kanál #bitcoin.cz na Freenode.
- Překládám Bitcoin Core do češtiny.
- Chvíli jsem těžil, o něco déle obchodoval. :c)
- Provozoval jsem bezpečnou bitcoinovou burzu BTCex.cz.
- Tvořím jak komerční, tak komunitní projekty.
- Na FI řeším problémy současných kryptoměn.

# Začalo to Bitcoinem

- 31. 10. 2008 – článek Satoshi Nakamota *Bitcoin: A Peer-to-Peer Electronic Cash System*
- leden 2009 – zahájení provozu bitcoinové sítě, Bitcoin 0.1
- 22. 5. 2010 – první komerční transakce (2 pizzy za 10k ฿)
- 17. 7. 2010 – vzniká burza Mt. Gox
- 18. 9. 2010 – slushův těžařský pool našel první blok
- konec 2010 – Satoshi Nakamoto „mizí“
- 9. 2. 2011 – parita s USD (1 ฿ = 1 $)
- 18. 4. 2011 – první fork: Namecoin

# Co dělá kryptoměnu kryptoměnou

- Použití asymetrické kryptografie k prokazování vlastnictví.
- Autonomní běh.
- Řízení algoritmy, ne centrální autoritou.
- Decentralizovaná povaha.
- Veřejná databáze všech transakcí (blockchain).

Bonusy:

- Nevratné transakce.
- Státem nezničitelný systém.
- Potenciálně anonymní peníze.

# Jak Bitcoin funguje

*Pohled uživatele*

- Mám jakousi bitcoinovou adresu pro příjem peněz (1Gx7EqWqoq6xTNKDFc5HWiz1ECNtWpubBo).
- Tu dám druhé straně, která mi má bitcoiny poslat.
- V bitcoinovém klientu uvidím nepotvrzenou příchozí transakci.
- Za chvíli jí začnou potvrzení pomalu nabíhat (cca 1 co 10 minut).
- Zhruba za hodinu se mi ukáže už jako potvrzená. Mám bitcoiny!
- Když budu chtít někde zaplatit, zkopíruji adresu příjemce do peněženky, zadám částku, dám poslat, odemknu heslem peněženku a platba se odešle.
- Po kontrolu se podívám na webu na svou adresu.
- Transakce tam sice je, ale posílá peníze ještě na nějakou jinou adresu, kterou neznám, stav je 0 Ƀ, i když v peněžence ty peníze vidím???

# Adresy

- Typická podoba: 1Gx7EqWqoq6xTNKDFc5HWiz1ECNtWpubBo
- Před nástupem těchto „adres“ se v bitcoinu peníze adresovaly na veřejné klíče.
- Adresa je kratší variantou – hashem se speciálním kódováním:

1. PubKey
2. Hash = RIPEMD160(SHA256(PubKey))
3. Checksum = první 4 bajty z SHA256d(verze ⊕ Hash)
4. **Address** = Base58(verze ⊕ Hash ⊕ Checksum)

- Do transakce se ale umístí jen *Hash*.
- Verze slouží k rozlišení různých typů, účelů (a kryptoměn).

# Jak Bitcoin funguje

*Technicky*

- Bitcoin je jako velká účetní kniha se záznamy odkud kam se převáděly peníze.
- Záznamy se shlukují do elementárních celků – transakcí.
- Transakce se zaznamenávají dávkově – po blocích.
- Bloky jdou za sebou a každý se odkazuje na ten předchozí
  → tvoří řetěz: *blockchain*

*Na počátku nebylo nic. „Budiž blok," pravil Satoshi. A stvořil genesis blok.*

# Bitcoin hlouběji: transakce

- Transakce má 2 části: **odkud** a **kolik kam**.
  - odkud = „vstupy“
  - kolik kam = „výstupy“
- Každý výstup kromě částky obsahuje také podmínky nutné pro jeho utracení – specifikované skriptem.
- Každý vstup ukazuje na nějaký neutracený výstup a dokládá splnění podmínek.
- Pokud suma vstupů > suma výstupů, tak rozdíl bude transakčním poplatkem.

# Skriptovací jazyk

- Turingovsky **ne**úplný (nemá cyklus).
- Odvozený od jazyka Forth – používá reverzní polskou notaci.

- konstanty (−1, 0, 1, …, 16)
- zásobníkové operace (přidávání, mazání, duplikace, prohazování, vyzobávání, …)
- větvení, kontrola vrcholku zásobníku, ukončení výpočtu, NOP
- aritmetické operace (+, −, neg, ++, −−, min, max, …)
- relační operátory (=, <, ≤, >, ≥, …)
- kryptografické operace (hashovací fce, ověření podpisu, ověření více podpisů)
- *zakázané:* řetězcové operace, bitové operace

# Programovatelné peníze

# Programovatelné peníze

- Typické skripty:
  - P2PK: `<sig> | <pubKey> OP_CHECKSIG`
  - P2PKH: `<sig> <pubKey> | OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
  - P2SH: `... {serialized script} | OP_HASH160 <scriptHash> OP_EQUAL`
- Lze ale téměř cokoli:
  - matematický výraz
  - vstup pro hash
  - DoS
  - ...

# Ukládání dat

- Fuj!
- I když se nám to nelíbí, lidé si cestu najdou…
  Např. zakódováním do adresy příjemce.

# Ukládání dat

- Fuj!
- I když se nám to nelíbí, lidé si cestu najdou…
  Např. zakódováním do adresy příjemce.
- Důsledek: zanášení množiny UTXO, která je typicky v RAM.

# Ukládání dat

- Fuj!
- I když se nám to nelíbí, lidé si cestu najdou…
  Např. zakódováním do adresy příjemce.
- Důsledek: zanášení množiny UTXO, která je typicky v RAM.
- Řešení: standardizace *OP_RETURN skriptu* pro až 40 B dat.
  - 40 B je dost na 32B hash + nějaký rozlišovací identifikátor.
  - Výstupy s tímto skriptem jsou z definice neutratitelné, proto nosívají nulovou částku.

# O úroveň výše: bloky

- Těžaři zvalidované transakce seskupují do bloků.
- Každý blok opatří razítkem *proof of work* (PoW).
  - PoW je založený na antispamové myšlence hashcash.
  - V Bitcoinu SHA256d.
  - Hash musí být menší než aktuální regulační hodnota, tzv. obtížnost.
  - Vytvořit validní blok tak je výpočetně náročné.
- Za svou práci si těžaři připíší odměnu ve formě
  a) transakčních poplatků ze všech transakcí v daném bloku,
  b) nové emise

  do tzv. coinbase transakce, která nemá žádné klasické vstupy.

# Jak se skládají transakce do bloku...

- Fyzicky: za sebe.
- Logicky: do Merklova stromu.
  - Každý vnitřní uzel je tvořen hashem hashů svých potomků.
  - Transakce jsou až v listech.
  - Pokud je potomek jen jeden, vezme se dvakrát.
- Jde o strukturu s řadou výhod, např.:
  - malý důkaz přítomnosti transakce v bloku,
  - možnost prořezávání stromu,
  - do hashe bloku se počítá jen kořenový hash Merklova stromu transakcí.

# ...a bloky do řetězce

- V záhlaví obsahuje každý blok hash toho předchozího (genesis blok samé nuly).
- Vytváří se tak kontinuální, nepřeskládatelná a nepřerušitelná kontinuita transakční historie.

# …a bloky do řetězce

- V záhlaví obsahuje každý blok hash toho předchozího (genesis blok samé nuly).
- Vytváří se tak kontinuální, nepřeskládatelná a nepřerušitelná kontinuita transakční historie.
- Čím je blok hlouběji, tím více výpočetní práce ho kryje.
  - K jeho modifikaci/nahrazení by bylo nutné znovu vytěžit i všechny bloky v řetězci nad ním.
  - Tedy čím je blok hlouběji, tím je i bezpečnější.
- Odtud i počet potvrzení transakce.

# Pro zajímavost srovnání výkonu

Nejvýkonnější superpočítač podle TOP500.org – Sunway TaihuLight: teoretický výkon **125.436 TFLOP/s** (10M6 jader, 15M3W spotřeba)

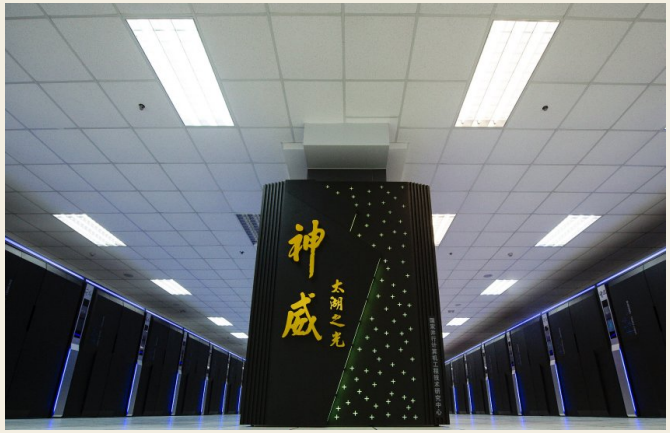
Výkon bitcoinové sítě: **21,2 ZFLOP/s** (1,67 Eh/s)

# Pro zajímavost srovnání výkonu

Nejvýkonnější superpočítač podle TOP500.org – Sunway TaihuLight: teoretický výkon **125.436 TFLOP/s** (10M6 jader, 15M3W spotřeba)

Výkon bitcoinové sítě: **21,2 ZFLOP/s** (1,67 Eh/s)

1 → kilo → mega → giga → tera → peta → exa → zetta → yotta




# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.
- Nezálohované klíče.

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.
- Nezálohované klíče.
- „Debianní klíče.“

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.
- Nezálohované klíče.
- „Debianní klíče.“
- „Konstantní náhoda.“

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.
- Nezálohované klíče.
- „Debianní klíče.“
- „Konstantní náhoda.“
- Slabá náhoda (Android: SecureRandom).

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.
- Nezálohované klíče.
- „Debianní klíče.“
- „Konstantní náhoda.“
- Slabá náhoda (Android: SecureRandom).
- Tvárnost (malleability) podpisů.

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.
- Nezálohované klíče.
- „Debianní klíče.“
- „Konstantní náhoda.“
- Slabá náhoda (Android: SecureRandom).
- Tvárnost (malleability) podpisů.
- Cloud…

# Různé problémy a zranitelnosti

- Útoky: 51%, Sybil, sociální inženýrství, …
- Peníze na serveru.
- Nešifrované úložiště klíčů.
- Nezálohované klíče.
- „Debianní klíče.“
- „Konstantní náhoda.“
- Slabá náhoda (Android: SecureRandom).
- Tvárnost (malleability) podpisů.
- Cloud…
- …

# Jak na klíče

*Generování*

- Praxe ukazuje, že nejspolehlivější je deterministické generování klíčů.
- Průkopníkem byl klient Electrum.
- Později standardizováno jako BIP0032.

# Jak na klíče

*Generování*

- Praxe ukazuje, že nejspolehlivější je deterministické generování klíčů.
- Průkopníkem byl klient Electrum.
- Později standardizováno jako BIP0032.
- **Další výhoda:** eliptické křivky umožňují generovat zvlášť veřejné klíče a zvlášť soukromé.

# Jak na klíče

*Uchovávání*

1. Vždy jedině šifrovaně.
2. Zálohovat!
3. Pozor na viry a malware…
4. Nenechávat na serveru.

- Off-line (air-gapped) počítač je dobrá cesta.
- Lze použít k tisku „papírové peněženky“.
- Kovová „peněženka“ na dlouhodobé skladování.
- Trezor.

# Bitcoinový Trezor

- Jednoduchý jednoúčelový počítač.
- Jediné místo, kde jsou dostupné soukromé klíče.
- Veškeré klíče se generují za běhu, ukládá se jenom semínko.
- Pro podepisování nepoužívá náhodná čísla.
- USB HID zařízení $\Rightarrow$ nejsou třeba ovladače.

# Limity anonymity

- Jednotlivá bitcoinová adresa (1…) či transakce vypadají anonymně…

  …a v bitcoinové síti jsou (byť pod Sybil útokem méně).
- Anonymitu snižuje např.:
  - recyklace adres,
  - slučování peněz z různých adres,
  - zveřejňování adresy se svou identitou/IP adresou.
- Analýza transakčních toků spolu s externími vstupy umí dosáhnout až deanonymizace.
  - Zejména shlukováním adres jednoho člověka.
  - Procházení pračkami/mixéry; CoinJoin Sudoku; BitIodine.
- WalletExplorer.com – projekt Aleše Jandy aka *kybl*a

# Snahy o lepší anonymitu

- CoinJoin – smícháme naše vstupy a výstupy!

# Snahy o lepší anonymitu

- CoinJoin – smícháme naše vstupy a výstupy!
- „Merge avoidance“ algoritmy pro volbu výstupů.

# Snahy o lepší anonymitu

- CoinJoin – smícháme naše vstupy a výstupy!
- „Merge avoidance“ algoritmy pro volbu výstupů.
- „Stealth addresses“ – odesílatel generuje cílovou adresu.

# Snahy o lepší anonymitu

- CoinJoin – smícháme naše vstupy a výstupy!
- „Merge avoidance“ algoritmy pro volbu výstupů.
- „Stealth addresses“ – odesílatel generuje cílovou adresu.
- „Reusable payment codes“ – vylepšená varianta SA.

# Snahy o lepší anonymitu

- CoinJoin – smícháme naše vstupy a výstupy!
- „Merge avoidance“ algoritmy pro volbu výstupů.
- „Stealth addresses“ – odesílatel generuje cílovou adresu.
- „Reusable payment codes“ – vylepšená varianta SA.
- Zero knowledge proofs → Zerocoin, Zerocash → z.cash.

# Snahy o lepší anonymitu

- CoinJoin – smícháme naše vstupy a výstupy!
- „Merge avoidance“ algoritmy pro volbu výstupů.
- „Stealth addresses“ – odesílatel generuje cílovou adresu.
- „Reusable payment codes“ – vylepšená varianta SA.
- Zero knowledge proofs → Zerocoin, Zerocash → z.cash.
- Novinka léta 2016: Mimblewimble.

# Mimblewimble

*Aneb všechno je jinak…*

- Anonymní odesílatel, příjemce i částka.
- Transakce existuje jen do doby, než se stane součástí bloku.
- Je ověřitelné, že součty neznámých částek sedí.
- Utracené výstupy můžete v klidu smazat.
- Podle autora by dnešní Mimblewimble-Bitcoin měl třetinový objem.

# Mimblewimble

*Aneb všechno je jinak…*

- Anonymní odesílatel, příjemce i částka.
- Transakce existuje jen do doby, než se stane součástí bloku.
- Je ověřitelné, že součty neznámých částek sedí.
- Utracené výstupy můžete v klidu smazat.
- Podle autora by dnešní Mimblewimble-Bitcoin měl třetinový objem.
- Cena: žádné skripty…

# Problém nafukování blockchainu

- Zcash na to trpí extrémně.
- „Řešením“ je Moorův zákon…
- Satoshi Nakamoto navrhl 2 řešení:
  a) prořezávání starých bloků,
  b) Simple Payment Verification.
- Klient Electrum přidává servery.
- Alternativním řešením je miniblockchain.

# Problém adres

- V kryptoměnách používané adresy jsou uživatelsky nepřívětivé.
- V anonymních kryptoměnách je to ještě horší.
- Žádné centralizované řešení se neuchytilo.

# Problém adres

- V kryptoměnách používané adresy jsou uživatelsky nepřívětivé.
- V anonymních kryptoměnách je to ještě horší.
- Žádné centralizované řešení se neuchytilo.
- Novinka 2016: **kryptoadresy**.
- Idea: využijme DNS k vybudování systému, jako je e-mail, který bude překládat aliasy michal@send.cash na původní adresy/identifikátory.
- Univerzální koncept i pro další aplikace s kryptografickými identifikátory (ale i třeba pro IBAN…).

# Platební kanály

- Chytré využití 2/2 multisig schématu.

# Platební kanály

- Chytré využití 2/2 multisig schématu.
- V rámci blockchainu se ustaví kanál s omezenou životností.

# Platební kanály

- Chytré využití 2/2 multisig schématu.
- V rámci blockchainu se ustaví kanál s omezenou životností.
- Jedna strana posílá malé částky peněz, druhá malé kousky protihodnoty.

# Platební kanály

- Chytré využití 2/2 multisig schématu.
- V rámci blockchainu se ustaví kanál s omezenou životností.
- Jedna strana posílá malé částky peněz, druhá malé kousky protihodnoty.
- Do blockchainu se uloží až uzavírající transakce.

# Platební kanály

- Chytré využití 2/2 multisig schématu.
- V rámci blockchainu se ustaví kanál s omezenou životností.
- Jedna strana posílá malé částky peněz, druhá malé kousky protihodnoty.
- Do blockchainu se uloží až uzavírající transakce.
- Platební kanály ve velkém = **lightning network**.

# Coincer

*Kryptoměny lze směňovat*

- Blockchainy jsou jako nezávislé databáze.
- Skripty ale umožňují vytvořit protokol pro atomickou směnu.
- **Nepotřebujeme žádnou třetí stranu.**
- Čistě P2P řešení s uspokojivou anonymitou.
- Proč? Dosavadní cracky burz čítají > 20 miliónů dolarů.

# Další aplikace

- Notářská razítka.
- Registr majetku (katastr, obchodní rejstřík, ...).
- Namecoin: DNS v blockchainu.
- Férová kasína.
  - SatoshiDice přímo nad blockchainem.
  - V hlavní roli statistika.
- BitMessage – anonymní zasílání zpráv.
- ...

# Výzva: Jak přeložit „blockchain“?

- Čeština ani slovenština nemají překlad pro „blockchain“.
- „Řetězec bloků“ se absolutně nechytl.
- Startuji iniciativu za český překlad.
- Idea: sesbírejme všechny návrhy, hlasujme a nejlepší vyberme.
- kybl pro věc věnuje doménu blockchain.cz.

# Výzva: Jak přeložit „blockchain“?

- Čeština ani slovenština nemají překlad pro „blockchain“.
- „Řetězec bloků“ se absolutně nechytl.
- Startuji iniciativu za český překlad.
- Idea: sesbírejme všechny návrhy, hlasujme a nejlepší vyberme.
- kybl pro věc věnuje doménu blockchain.cz.
- **Teď:** kdo naprogramuje podpůrný web? :c)

# V kryptoměnách je budoucnost!