fabhack

brmlab
hackerspace prague

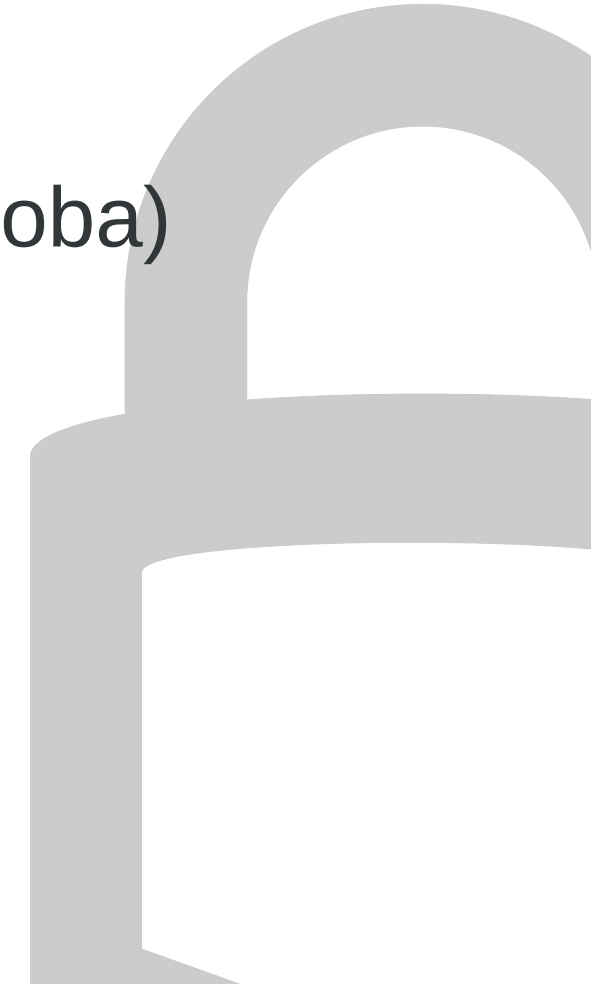
BITCOINCZ

slush & stick

- slush:
  - “Vynálezce” mining poolů, designér Stratum protokolu a provozovatel poolu mining.bitcoin.cz
  - Člen týmu Electrum
- stick:
  - Hacker a technologický nadšenec
  - spoluzakladatel Brmlab hackerspace

Tým

- Marek “slush” Palatinus
- Pavol “stick” Rusnák
- LionLuck (CNC guru)
- ostatní (marketing, bezpečnost, výroba)
- VY! (open-source)



brmlab

- Pražský hackerspace
- založen 2010
- Cca 50 členů
- Pravidelné úterní večery
- Bitcoin Conference 2011 afterparty
- Nepravidelné Bitcoin semináře (nejbližší 11.04.2012)
- http://brmlab.cz/

Překážky všeobecného rozšíření Bitcoinu

- Bezpečnost uživatelského počítače
  - malware, veřejně přístupné (nedůvěryhodné) počítače, upravení bitcoin klienti
- Ztráta peněženek
  - Selhání HW, reinstalace počítačů, přepsání dat
- Mobilita plateb
  - Uživatel musí být online

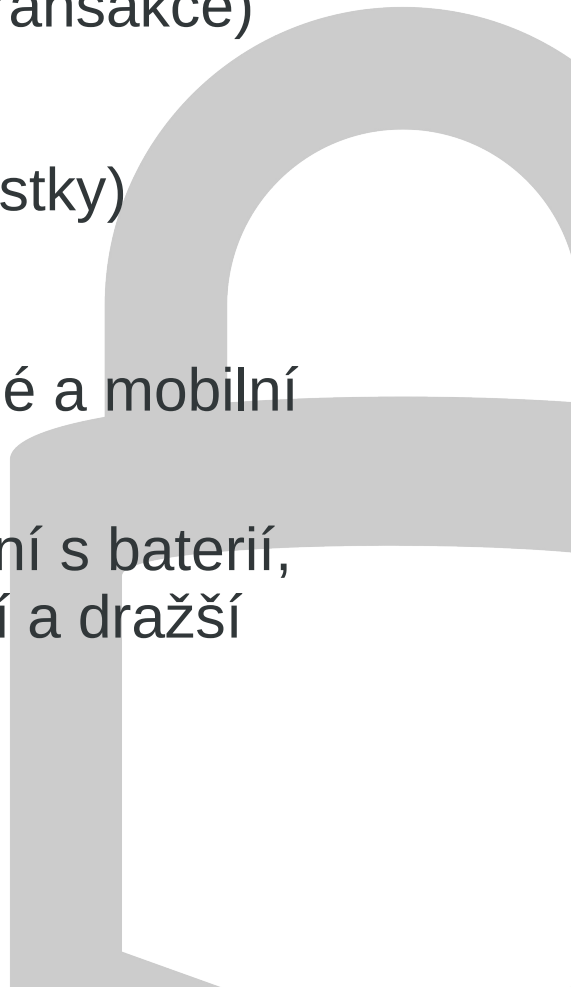
- Typické “bezpečné” řešení peněženky:
  - instalace bitcoin klienta na USB disk s Linuxem a privátními klíči vytištěnými na papír
  - Nevhodné pro běžnou populaci, nepohodlné, náchylné k chybám

Dostali jsme nápad

- Vytvořit zařízení, které:
  - Umožní bezpečně vytvářet transakce na libovolném počítači (Internetová kavárna, počítač u kamaráda)
    - Zařízení ke své funkci stále potřebuje počítač, cílem je primárně zajistit bezpečnost, nikoliv “opravdovou” mobilitu
  - Oddělí privátní klíče (“peněženku”) od bitcoin software
  - Skryje před uživatelem přebytečnou komplexnost správy privátních klíčů
  - Nabídne jednoduché papírové (offline) zálohy peněženky
  - Zpřístupní peněženku, aby ji měl uživatel vždy po ruce

KISS

- USB dongle
  - Bez baterie (napájen přes USB)
  - Bez internetového připojení (pouze podepisuje transakce)
  - Bez klávesnice (jenom tlačítka ano/ne)
  - S displejem (pro kontrolu správnosti adresy a částky)
- Poučili jsme se z chyb ostatních:
  - Snaha vytvořit samostatné zařízení pro bezpečné a mobilní platby
  - Pokusy skončily vytvořením komplexního zařízení s baterií, klávesnicí, displejem, fotoaparátem a wifi = horší a dražší napodobenina čínského mobilního telefonu :-)



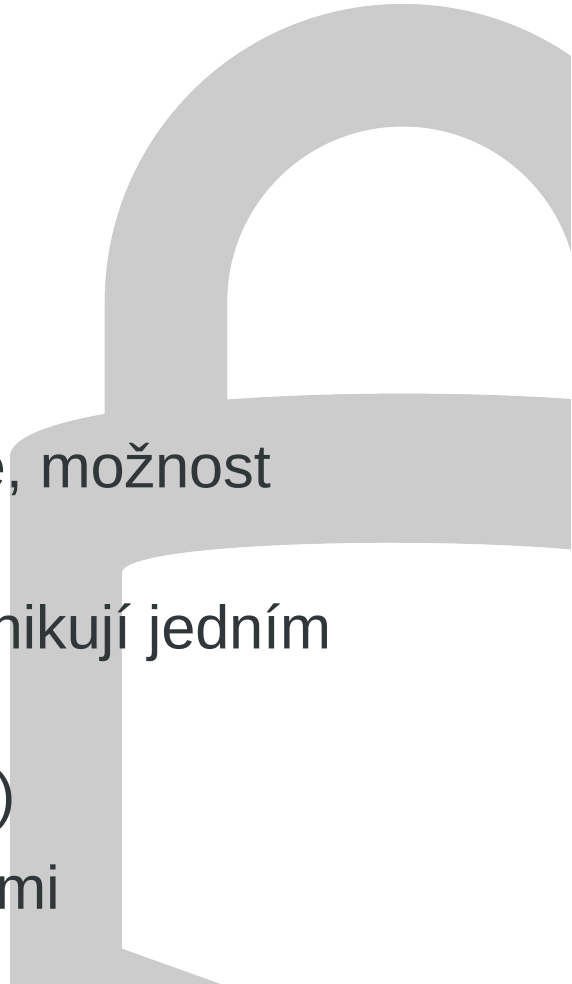
TREZOR – dvě verze

Pro hackery a nadšence

Pro Vaše prarodiče

TREZOR – dva formáty

- Raspberry Pi + Trezor shield
  - firmware napsaný v Pythonu
  - Raspberry Pi
  - Otevřený komunitě, vhodný na prototypování
- Bitcoin Trezor
  - firmware napsaný v C/C++
  - ARM microcontroller (Cortex M3)
  - Zaměřený na bezpečnost pro koncové uživatele, možnost nahrání pouze digitálně podepsaného firmware
- Obě zařízení s počítačem a bitcoin software komunikují jedním protokolem
  - USB HID (bez nutnosti instalace ovladačů v OS)
  - Klientský software nepozná rozdíl mezi zařizeními



První start (nebo reset zařízení)

- Uživatel zvolí, zda se má používat ochrana PIN
  - A pokud ano, rovnou ho nastaví
- Uživatel zvolí, zda se má používat ochrana pomocí OTP
- Zařízení vygeneruje seed a na displeji zobrazí (poprvé a naposledy!) tzv. “seed mnemonic” (Electrum, BIP-0032):

  “odd million spirit behind beyond scar

  numb clean made truck shelter some”

  - Uživatel je vyzván, aby větu opsal na papír a uchoval na bezpečném místě

Podepisování transakcí

- Na displeji se zobrazí první adresa a částka
  - Uživatel může tlačítky buď adresu potvrdit nebo stornovat celou transakci
- Na displeji se zobrazí druhá adresa a částka
  - Uživatel může tlačítky buď adresu potvrdit nebo stornovat celou transakci

…

- Pokud je nastaveno, zobrazí se OTP (a uživatel je případně dotázán na PIN)
  - Uživatel transakci potvrdí opsáním OTP a zadáním PINu na klávesnici počítače.
  - Pokud OTP a PIN souhlasí, do počítače je odeslána podepsaná bitcoinová transakce

Bitva na více frontách

- Bitcoin Trezor
  - hardware
  - firmware
  - obal
- Trezor shield
  - hardware
  - firmware
- Podpora v klientech
  - Electrum, MultiBit, Armory, …
- Bezpečnostní audit, design, výroba, distribuce, podpora atd.

Děkujeme za pozornost!

http://bitcointrezor.com/