OpenLab

Cryptocurrencies

Petr Švenda

svenda@fi.muni.cz @rngsec

Faculty of Informatics, Masaryk University, Czech Republic

CROCS
Centre for Research on Cryptography and Security

The plan

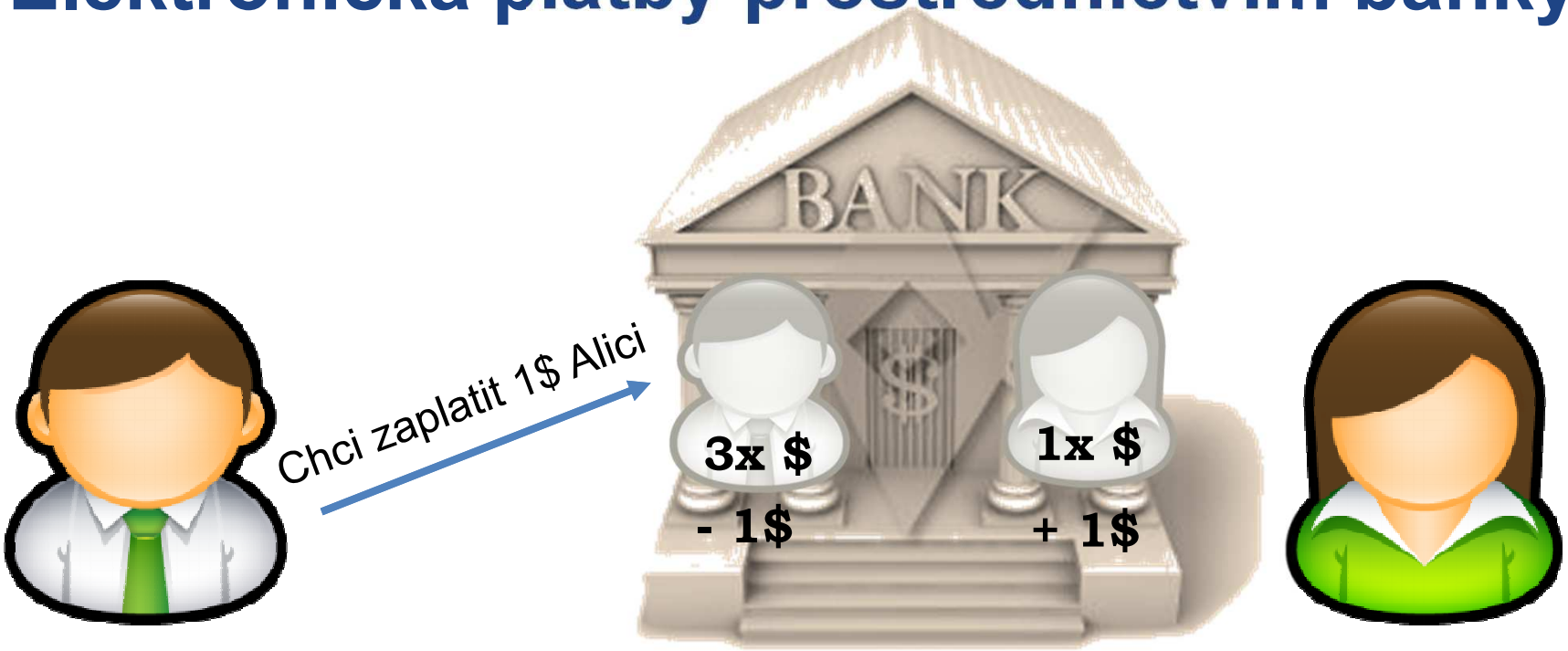
- Motivation and basics of Bitcoin operations
- Alternative cryptocoins to Bitcoin and why
- Make your own transaction

APOLOGY FOR CZECH LANG SLIDES – NOC VĚDCŮ ☺ (SEE ADDITIONAL SLIDES)

Hotovostní platby

- Ochrana soukromí
- Zaplacenou minci nelze použít znovu

Elektronická platby prostřednictvím banky



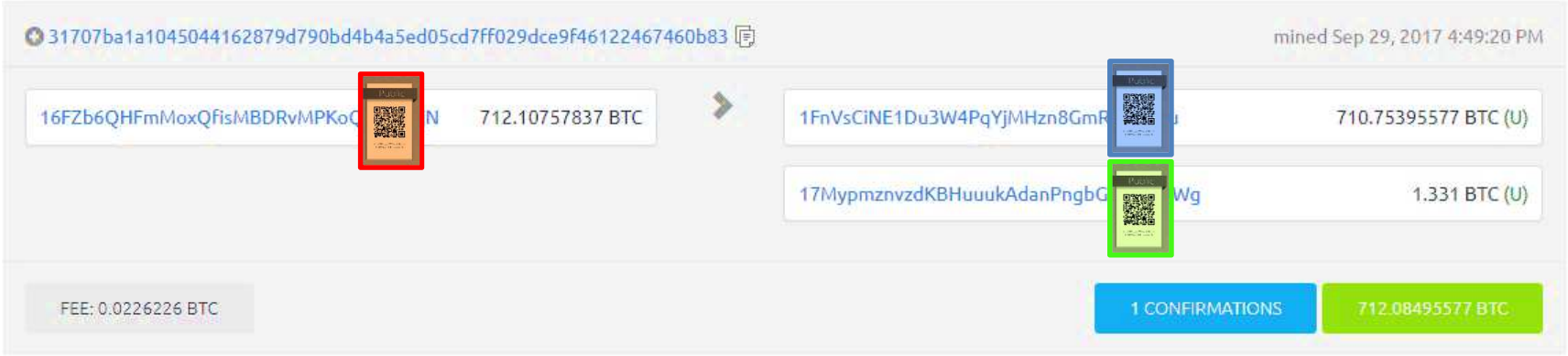
- Lze bezhotovostně a na „dálku“
- Co když Alice nemá účet u stejné banky?
- Co když banka začne podvádět?

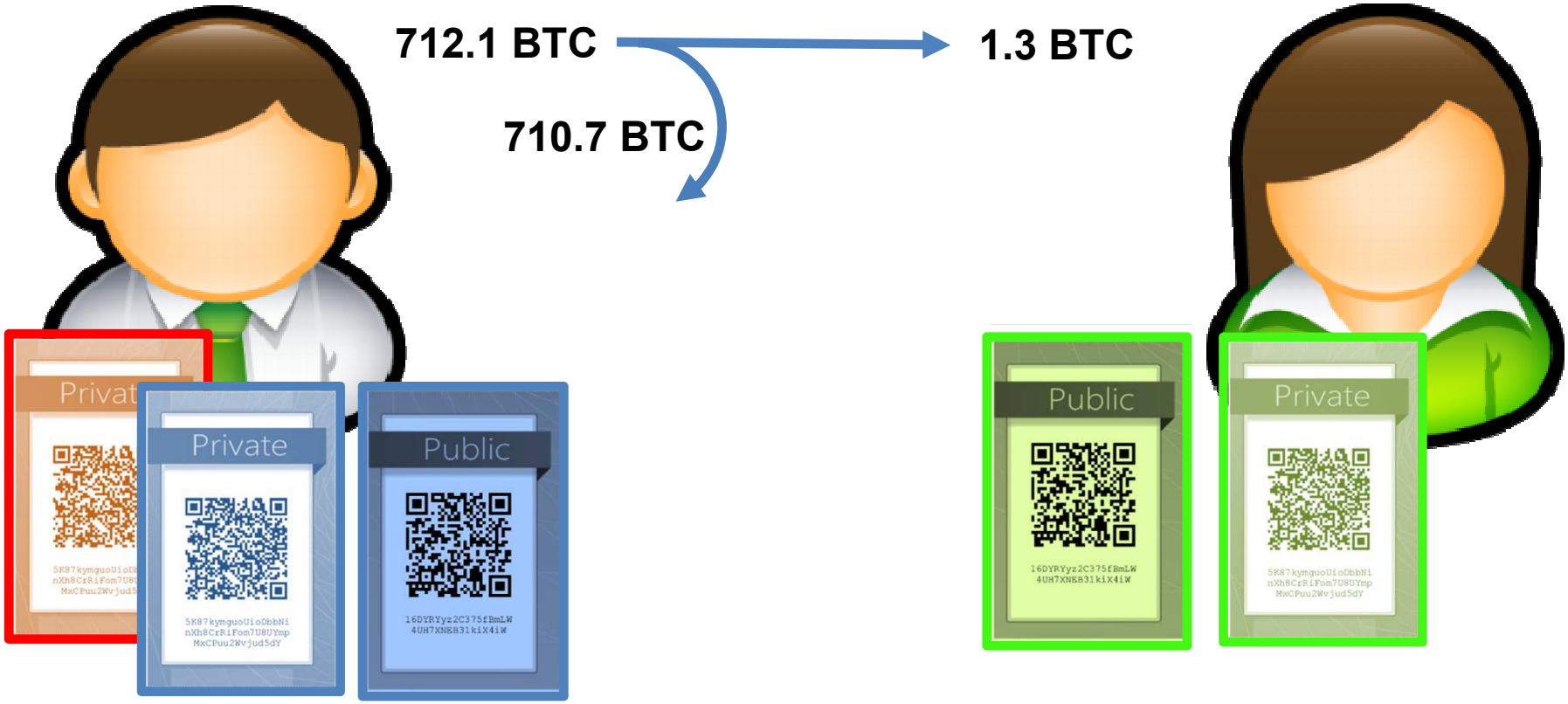
Ideální elektronický převod a konto

- Rychlý převod (ideálně sekundy)
- Malé nebo žádné poplatky
- Soukromí (aby ostatní nevěděli, kolik máme)
- Nezávislost na centrální bance (hyper)-inflace
- Nemožnost padělat mince
- Snadné cestování s majetkem (ne kilogramy zlata ☺)
- …

Digitální kryptografické měny - idea

1. Veřejná adresa a platební klíč (veřejný/privátní klíč)
   – Typicky 256b ECC
2. Kdo vlastní podepisovací klíč k adrese, ten může platit (provést transakci)
3. Veřejný seznam všech transakcí aby nešlo platit dvakrát (blockchain)
4. Náročný výpočet pro nový blok
   – Aby nebylo nutné mít centrální autoritu


31707ba1a1045044162879d790bd4b4a5ed05cd7ff029dce9f46122467460b83
mined Sep 29, 2017 4:49:20 PM
16FZb6QHFmMoxQfisMBDRvMPKoQ
N
712.10757837 BTC
1FnVsCiNE1Du3W4PqYjMHzn8GmR
710.75395577 BTC (U)
17MypmznvzdKBHuuukAdanPngbG
Wg
1.331 BTC (U)
FEE: 0.0226226 BTC
1 CONFIRMATIONS
712.08495577 BTC


712.1 BTC
710.7 BTC
1.3 BTC
Private
Private
Public
Public
Private

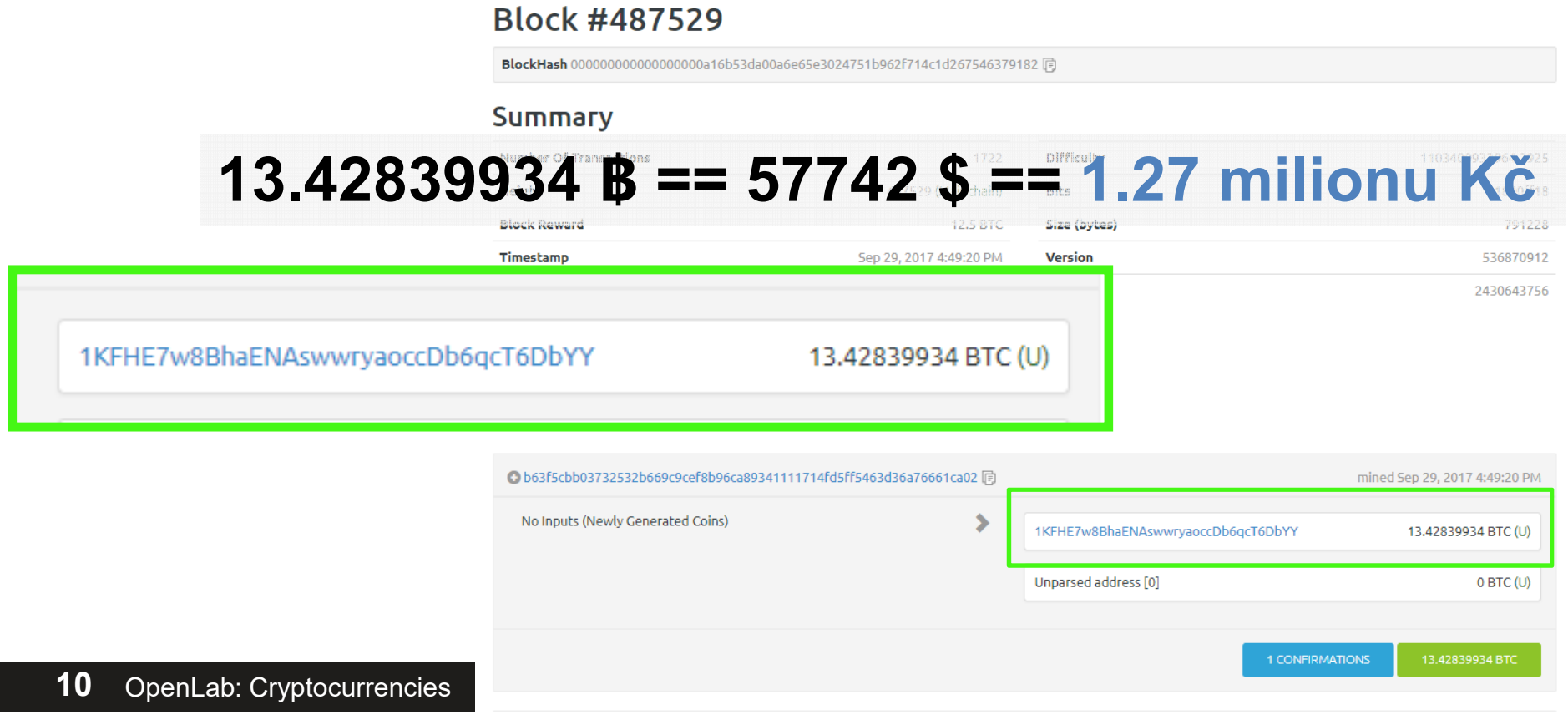
Semínko		SHA256(blok)
12345	→	3948 23840
94302	→	0439 91254
66439	→	5484 98573
…		
93204	→	000048573

SHA256(blok) == ‘0000xxxxx’ ?

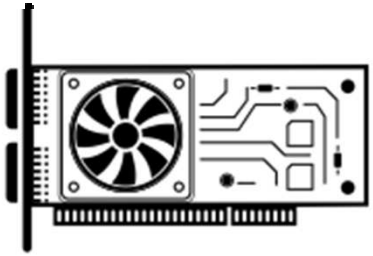
- Jak zamezit dodatečné změně bloku s transakcemi?
- Digitální podpis nelze použít – nemáme banku
- Digitální těžaři (miners) se snaží vyřešit kvíz!

Proč investovat energii do těžení?

- Kdo první vyřeší kvíz, dostane 12.5 bitcoinů (฿)
- Navíc poplatky za zařazené transakce (+1฿)



Jak rychle počítat hash SHA256?



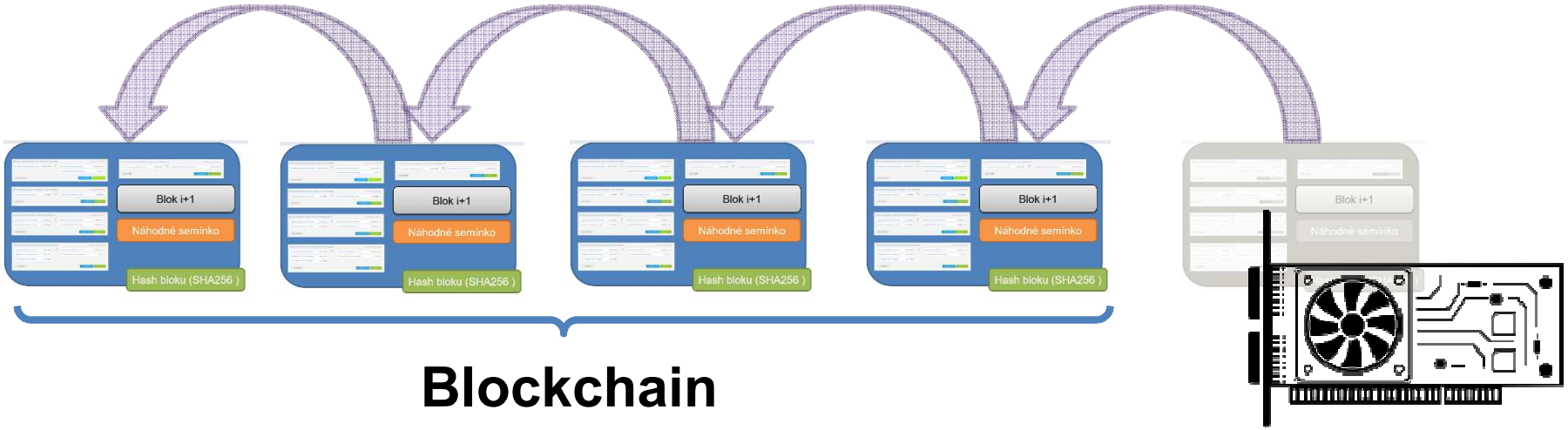
A těžaři počítají opravdu hodně!

- Počet hash za sekundu: 10 000 000 000 000 000
  - Zcela náhodné 8 znakové heslo by uhodli za 1 sekundu
  - Správný blok nalezen jen jednou za 10 minut (těžké!)
- Spotřeba elektrické energie 18.4 TWh / rok
  - Asi jako celé Chorvatsko nebo 25% České republiky
  - Temelín na plný výkon

https://digiconomist.net/bitcoin-energy-consumption

Všechny bloky jsou veřejné (blockchain)

- Jednotlivé bloky s transakcemi jsou provázané
- Tvoří veřejnou historii všech provedených transakci
- Každý si může zkontrolovat platnost transakce
  - Snadné, stačí ověřit hash na bloku a podpis na transakci

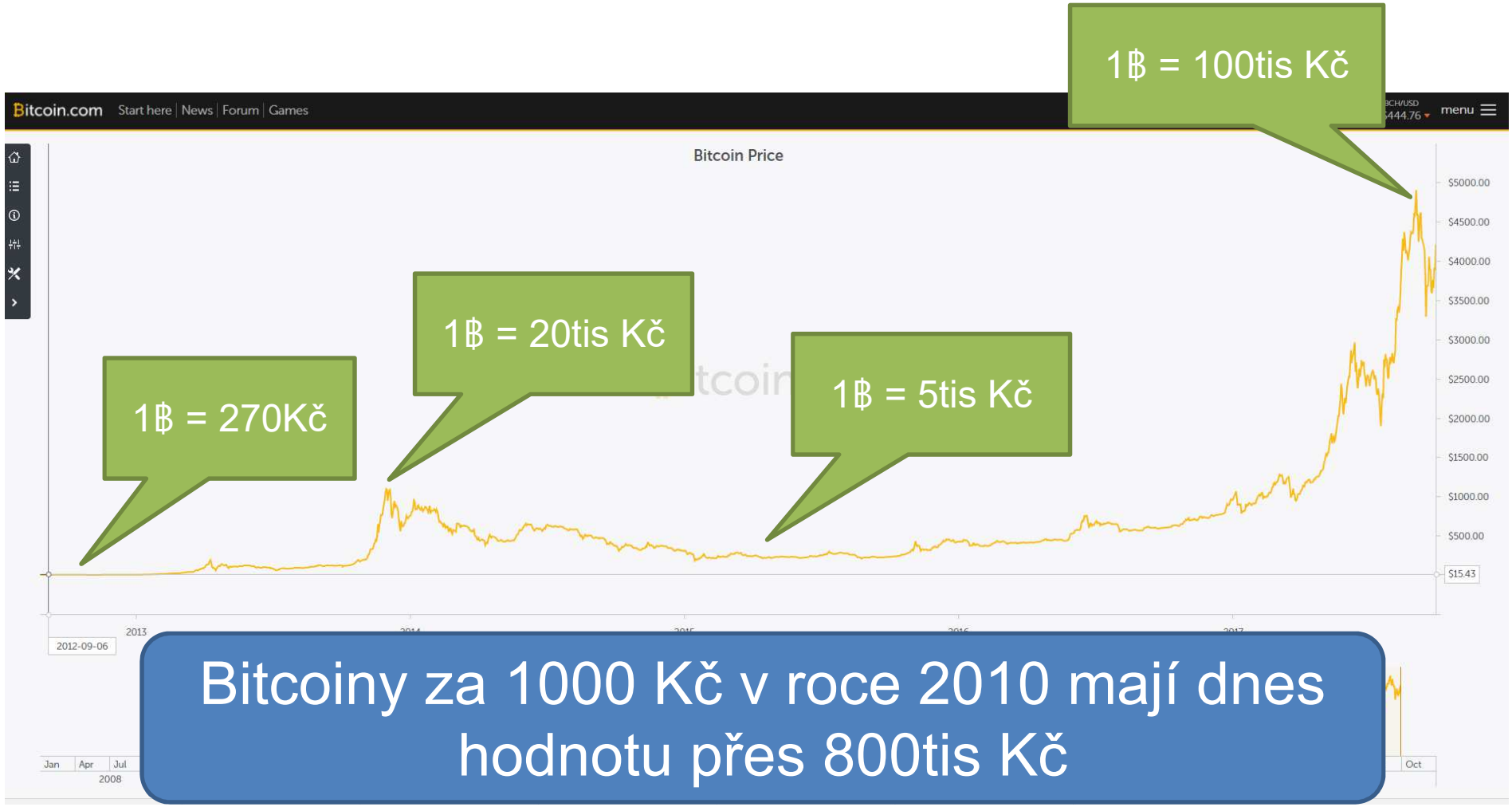


Jak si udělat digitální peněženku?

- Papírová
- Aplikace na mobilním telefonu
  - Coinomi, JAXX
- Čipová karta (Ledger nano)
- Burzy (použití při obchodování)

- Jak získat digitální peníze?
  - Nákup bitcoinů v bankomatu (Omega, Vaňkovka)
    - Následně směna za libovolnou kryptoměnu
  - Převodem Kč na burzu, nákup vybrané kryptoměny

Má to cenu?



Bitcoiny za 1000 Kč v roce 2010 mají dnes hodnotu přes 800tis Kč

Other cryptocurrencies (altcoins)

- Why something else than Bitcoin?

1. Cost of transaction
   - >$2 at the moment (for every transfer)
2. Time to confirm transaction (+ limited block size)
   - 4 blocks inside chain commonly required, ~10 minutes per block
3. Traceability (anonymity) of transactions
   - Source, destination and amount is public
4. Centralization of computation
   - China mining rigs with ASICs
5. Limited scripting language
   - For more complicated smart contracts

Other cryptocurrencies (altcoins)

- Copycats
  - Take Bitcoin's source code and change the name and icon
  - E.g., Litecoin (but LTC is now adding new features before Bitcoin)
- Bitcoin-style, but adding some distinct features
  - Ethereum: Turing-complete scripting for smart contracts, proof-of-ownership
  - Zcash: zero-knowledge proof for sender/receiver/amount (shielded transactions), ASIC-resistant proof of work (large memory required)
  - Monero: private transactions via mixing
- More traditional styles (Ripple, NEM), focused on banks
  - decentralized network of verification nodes (faster and cheaper txs)
  - but less privacy and overall resilience against central control
- Initial Coin Offerings (ICO)
  - Basically crowdfunding campaign (often via Ethereum smart contracts)
  - Frequently scam, recently banned by China

Mo

WorldCoinIndex

Home | Trending | Overview | 24 volume | Exchanges | Tools | ICO | Portfolio | USD | Search cryptocoin | Logout

#	Name	Ticker	Last price	%	24 high	24 low	Price Charts 7d	24 volume	# Coins	Market cap
1	Bitcoin	BTC	$ 4,323.4578	+2.34%	$ 4,340.6124	$ 4,148.0907		$ 664.48M	16.60M	$ 71.79B
2	Ripple	XRP	$ 0.2320411	+8.85%	$ 0.2361276	$ 0.2129615		$ 302.96M	38.34B	$ 8.89B
3	Bitcoincash	BCH	$ 358.491076	+0.33%	$ 373.008767	$ 345.202630		$ 188.87M	16.49M	$ 5.91B
4	Ethereum	ETH	$ 294.706969	+0.82%	$ 295.699991	$ 287.864513		$ 176.07M	94.96M	$ 27.98B
5	Qtum									
6	Litecoir									
7	Neo									
8	Zcash									
9	Etherei									
10	Dash									
11	Monerc									
12	Omiseg									

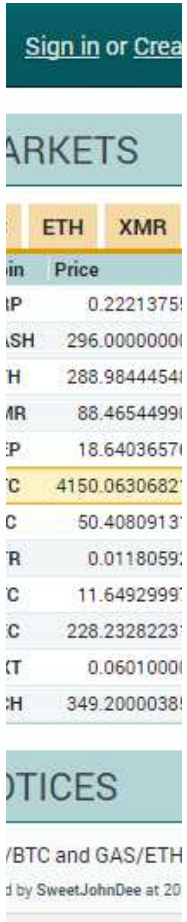
WorldCoinIndex

Home | Trending | Overview | 24 volume | Exchanges | Tools | ICO | Portfolio | USD | Search cryptocoin | Logout

#	Name	Ticker	Last price	%	24 high	24 low	Price Charts 7d	24 volume	# Coins	Market cap
701	Carpediem	DIEM	$ 0.0000115	0.00%	$ 0.0000115	$ 0.0000115				
702	Devcoin	DVC	$ 0.0000101	0.00%	$ 0.0000101	$ 0.0000101			10.54B	$ 106,771
703	Neucoin	NEU	$ 0.0000092	0.00%	$ 0.0000092	$ 0.0000092			216.33M	$ 1,980
704	Xencoin	XNC	$ 0.0000007	0.00%	$ 0.0000007	$ 0.0000007			170.56M	$ 120

← Previous 100

Crypto trading



Hands on - SysCoin

- Why Syscoin?
  - Probably a “shit” coin (but good for experiments)
  - Cheap coin ($0.15/SYS), very low transaction fee
  - New block every minute (so we don’t need wait long)
  - Principles same as for the more expensive currencies
- Generate own wallet
  - Paper wallet: https://WalletGenerator.net
    - Ideally download from GitHub, run offline via LiveCD…
  - Mobile wallet (Coinomi Android)
    - Generate new public key (Receive)


WalletGenerator.net
Universal Open Source Client-Side Wallet Generator
Choose currency : Syscoin
Single Wallet
Paper Wallet
Bulk Wallet
Brain Wallet
Wallet Details
Support
BIP38 Encrypt?
Passphrase:
Randomly generate
OR
Enter your own WIF private key
Apply »
Print
Private
Public
To deposit funds to this paper wallet, send cryptocurrency to its public address, anytime.
Verify your balance by searching for the public address using a blockchain explorer such as blockchain.info.
DO NOT REVEAL THE PRIVATE KEY until you are ready to import the balance on this wallet to a cryptocurrency client, exchange or online wallet.
Amount :
Date :
Notes :
Support WalletGenerator.net
Download (GitHub Repository)
@WalletGenerator
Copyright WalletGenerator.net. JavaScript copyrights are included in the source. No warranty.

Hands on – SysCoin II.

1. I will send some SYS to your wallet
2. Resend some fraction to your friend(s)
3. Observe your transaction(s) at https://chainz.cryptoid.info/sys/
   - Can you find your transaction?
   - Can you figure out Dusan's initial amount of SYS?
   - Can you figure out my initial amount of SYS?
   - Can you figure out how I obtained my SYS?
   - Can you track other's transactions?
   - Can you decide if output transaction was already spend?

What next?

1. Just enjoy the knowledge ☺
2. Possibly buy some (small) amount of Bitcoins (ATM) and investigate the options
3. Play with some virtual portfolio – e.g., https://www.worldcoinindex.com/portfolio
   – Create virtual set of favourite coins and observe gain/loss
4. Possibly register on some exchange
   – Kraken, Coinbase…