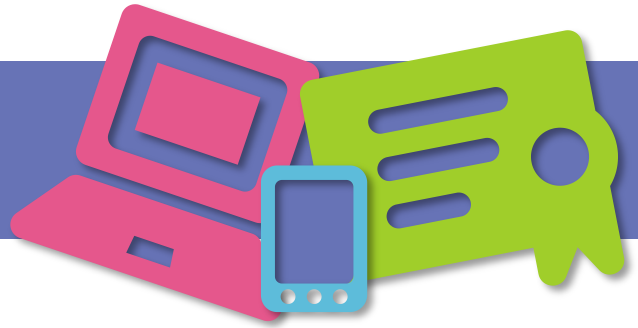
SECURITY 2015

23. ročník konference o bezpečnosti v ICT



Bitcoin

Ing. Adam Brunai

AEC, spol. s r.o.

History of money

Bartering

Coins

Fiat money

Bitcoin

Metals

Paper money

PayPal

PayPal

< 5 000 BC 600 BC 1000 1971 1998 2008

Fiat money

- Backed solely by the authority of a governing body and the trust of the public
- Currently, the main payment method in almost every country

Bitcoin

- First decentralized **cryptocurrency**
- What is the difference between **bitcoin** and the **other existing payment systems**?
  - Independent from fiat money
  - Independent from user's country
  - Decentralized
  - Low transaction fees (0.5 CZK)

Who accepts bitcoin?

amazon.com

DELL

SUBWAY

Microsoft

TESLA

WordPress

Wikipedia
The Free Encyclopedia

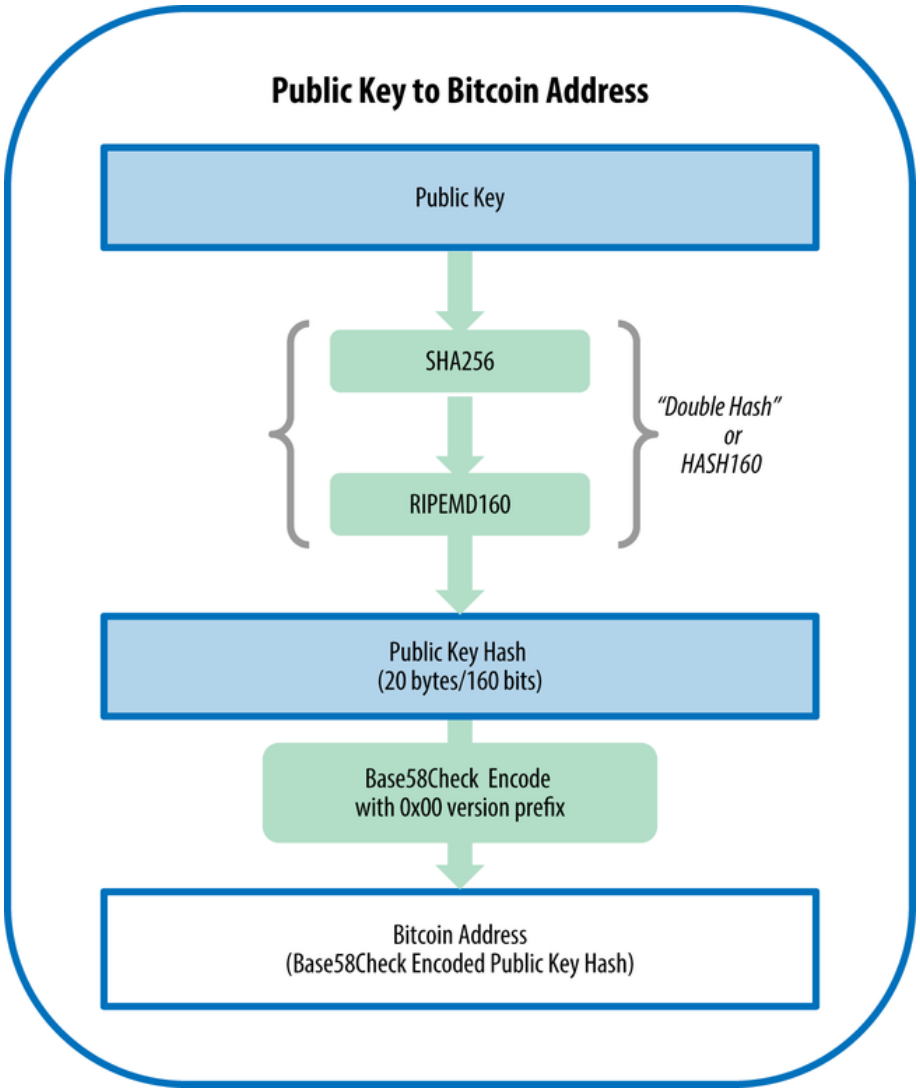
Victoria's Secret

And many more...

Address

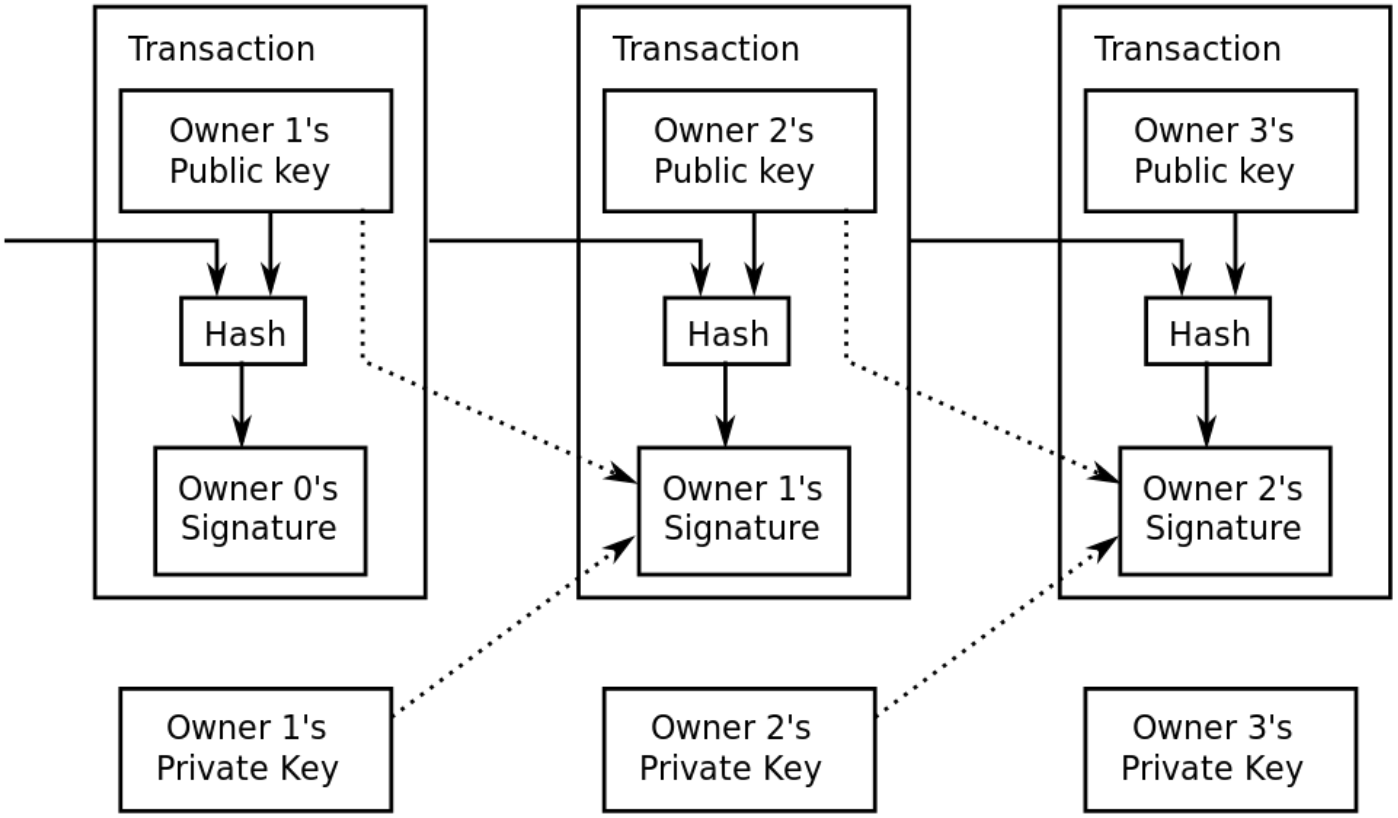
- **Unique identifier** of transaction recipient based on ECDSA public and private key pair
- Abstraction of **bank account**
- It is possible to generate **unlimited amount** of bitcoin addresses
- An example of bitcoin address:
  `3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy`

Address


Public Key to Bitcoin Address
Public Key
SHA256
RIPEMD160
"Double Hash"
or
HASH160
Public Key Hash
(20 bytes/160 bits)
Base58Check Encode
with 0x00 version prefix
Bitcoin Address
(Base58Check Encoded Public Key Hash)

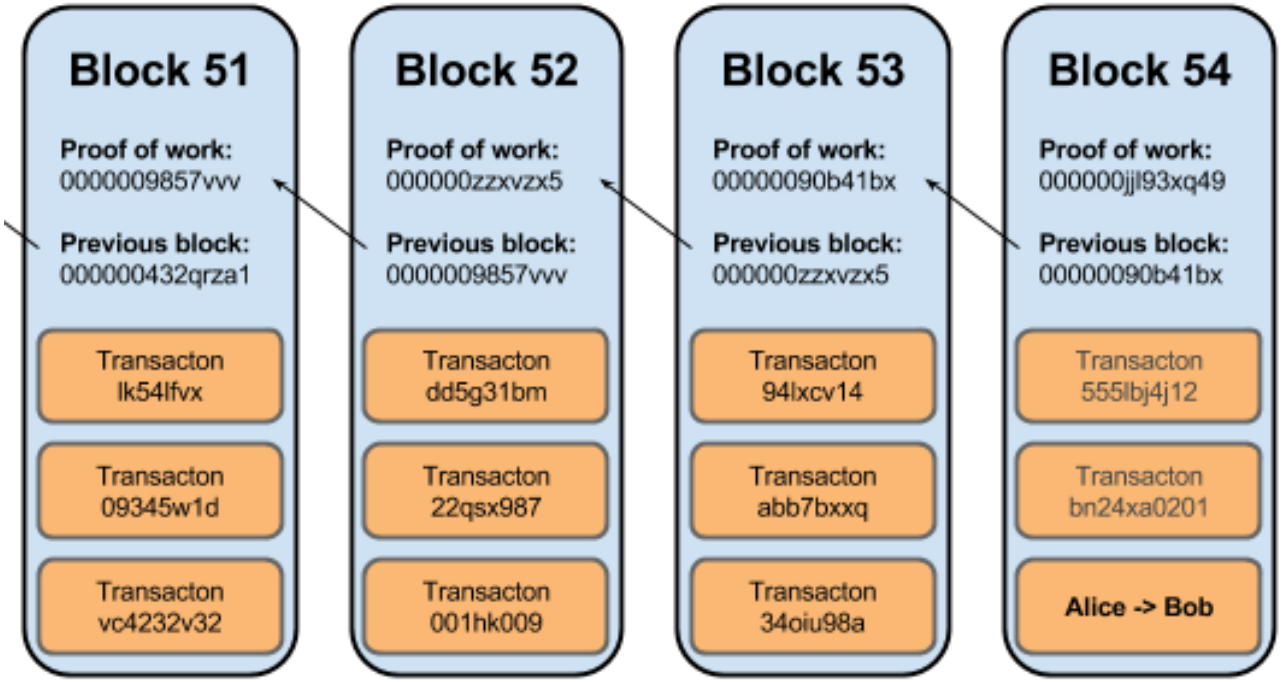
Transaction

- Transfer of bitcoins from a bitcoin address to another address



Block chain

- Winner of proof of work lottery is allowed to add new block of transactions to the **block chain** and get a reward in a form of bitcoins



Proof of work

- Find *x* such that $hash(c||x) < target$
- Let $c =$ "Hello, world!" and $target = 2^{224}$, then:

```
"Hello, world!0" → 1312af178c253f84028d480a6adc1e25e8...
"Hello, world!1" → e9afc424b79e4f6ab42d99c81156d3a172...
"Hello, world!2" → ae37343a357a8297591625e7134cbea22f...
...
"Hello, world!4248" → 6e110d98b388e77e9c6f042ac6b497c...
"Hello, world!4249" → c004190b822f1669cac8dc37e761cb7...
"Hello, world!4250" → 0000c3af42fc31103f1fdc0151fa747...
```

$$\boxed{x = 4250}$$

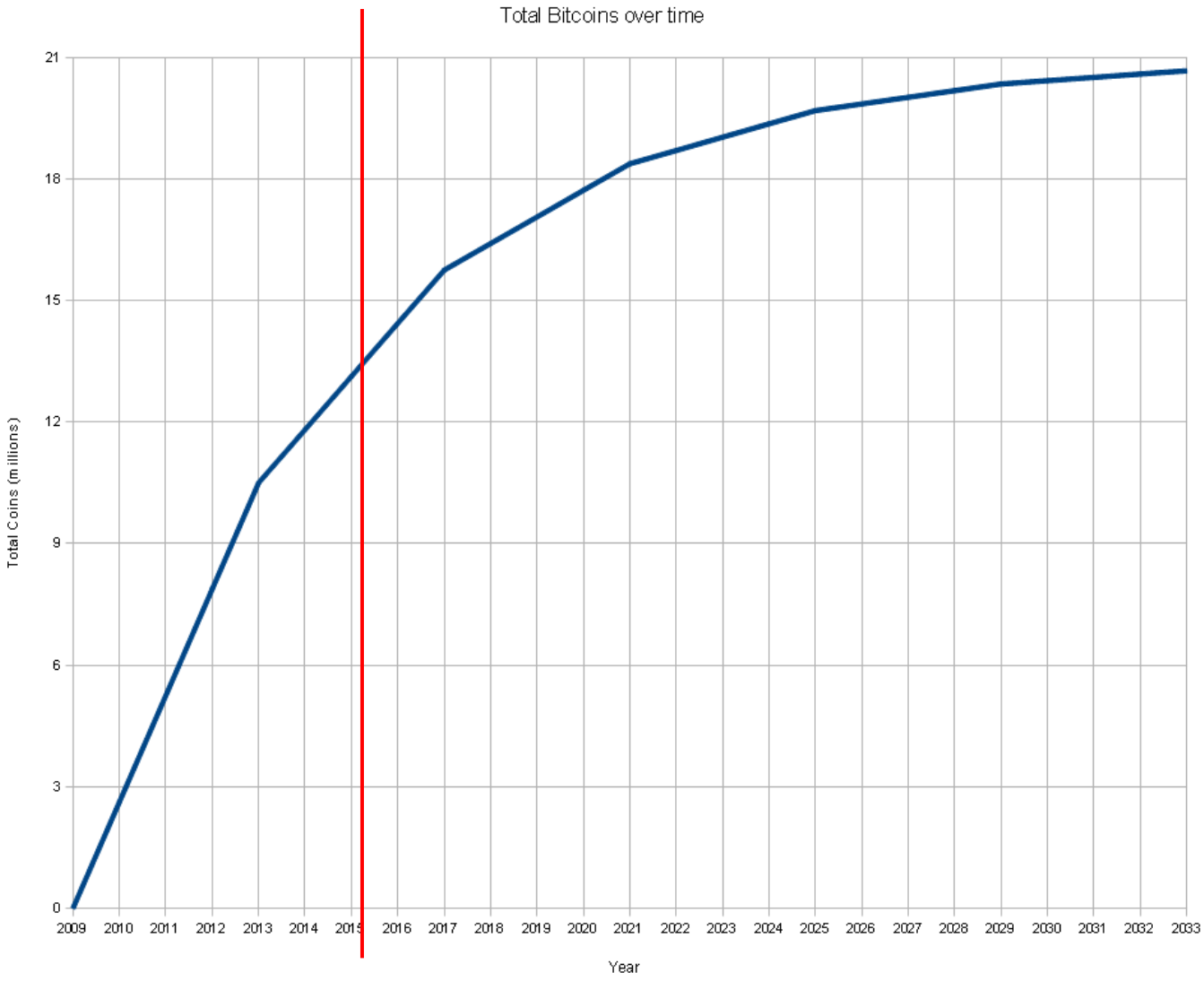
Mining

- Every block creates 50 BTC. This value halves every 210 000 blocks. Therefore, maximal amount of available bitcoins is the sum of the geometric series :

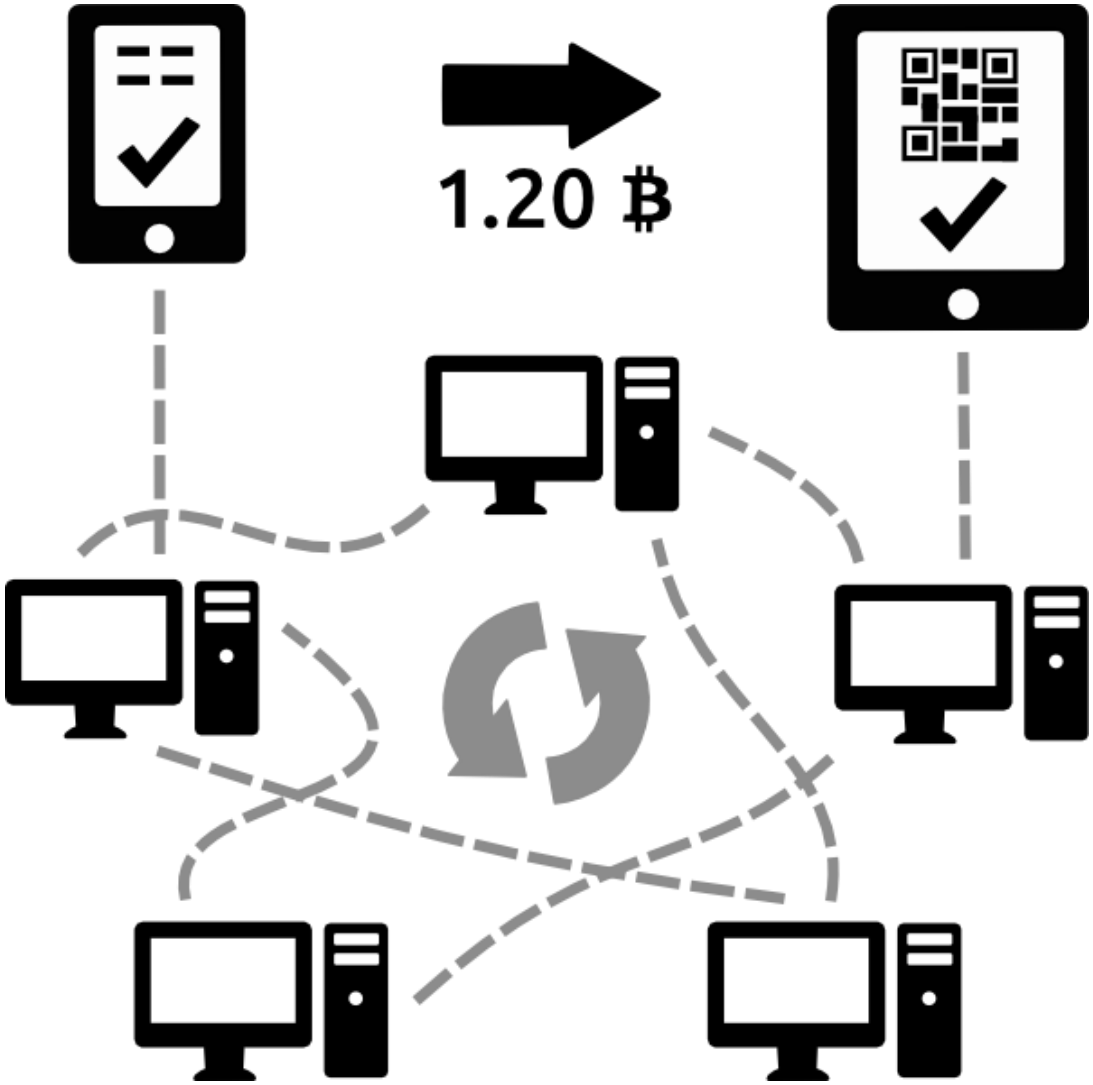
$$\sum_{n=0}^{\infty} \frac{210\,000 \cdot 50}{2^n} = 210\,000 \cdot 50 \cdot \frac{1-0}{1-0.5} = 21\,000\,000\ BTC$$

- ~ 13 840 400 BTC = 77 703 404 802 CZK have been mined until today

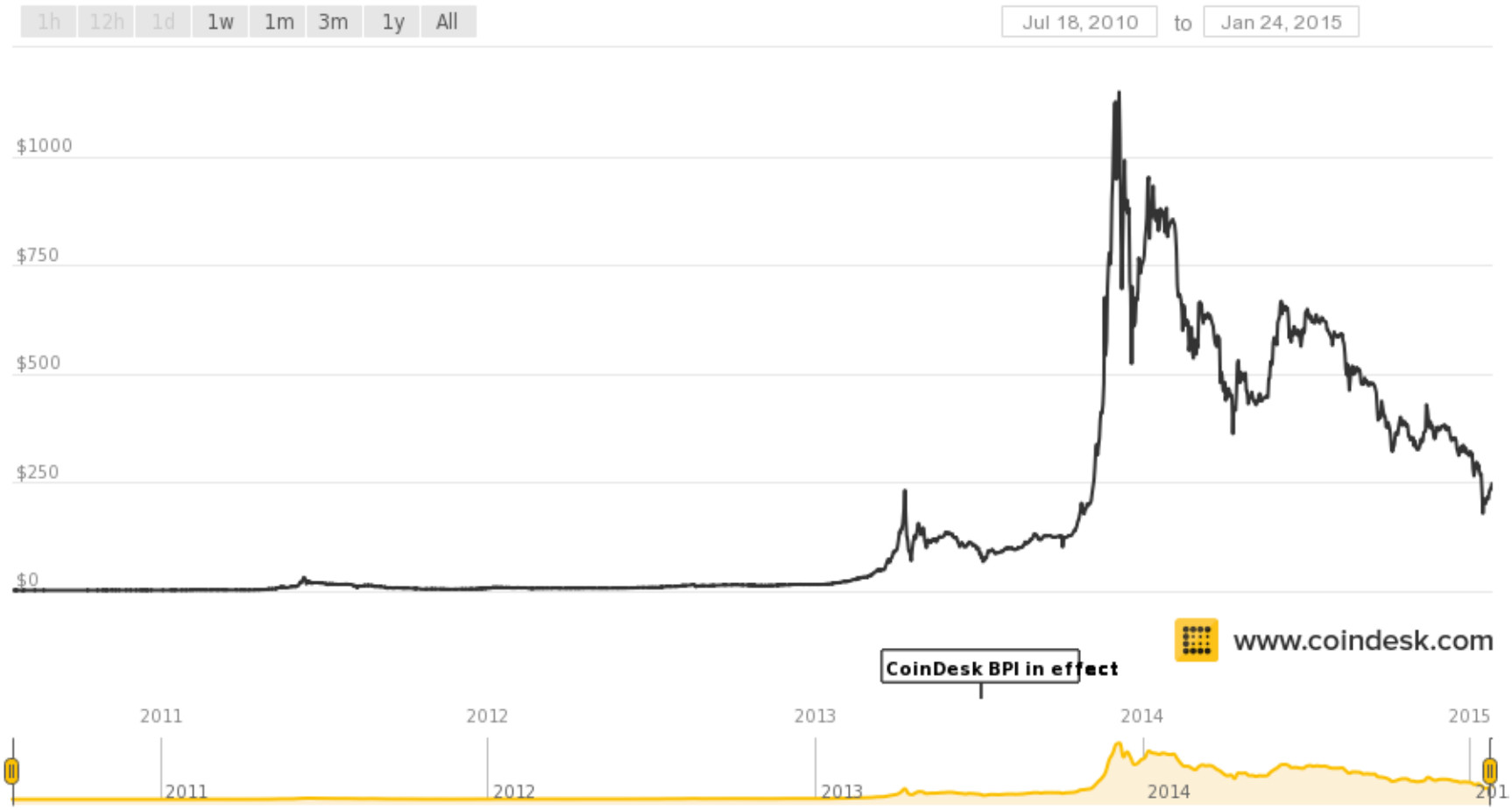
Mining


Total Bitcoins over time
Total Coins (millions)
0
3
6
9
12
15
18
21
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
Year
today

P2P network

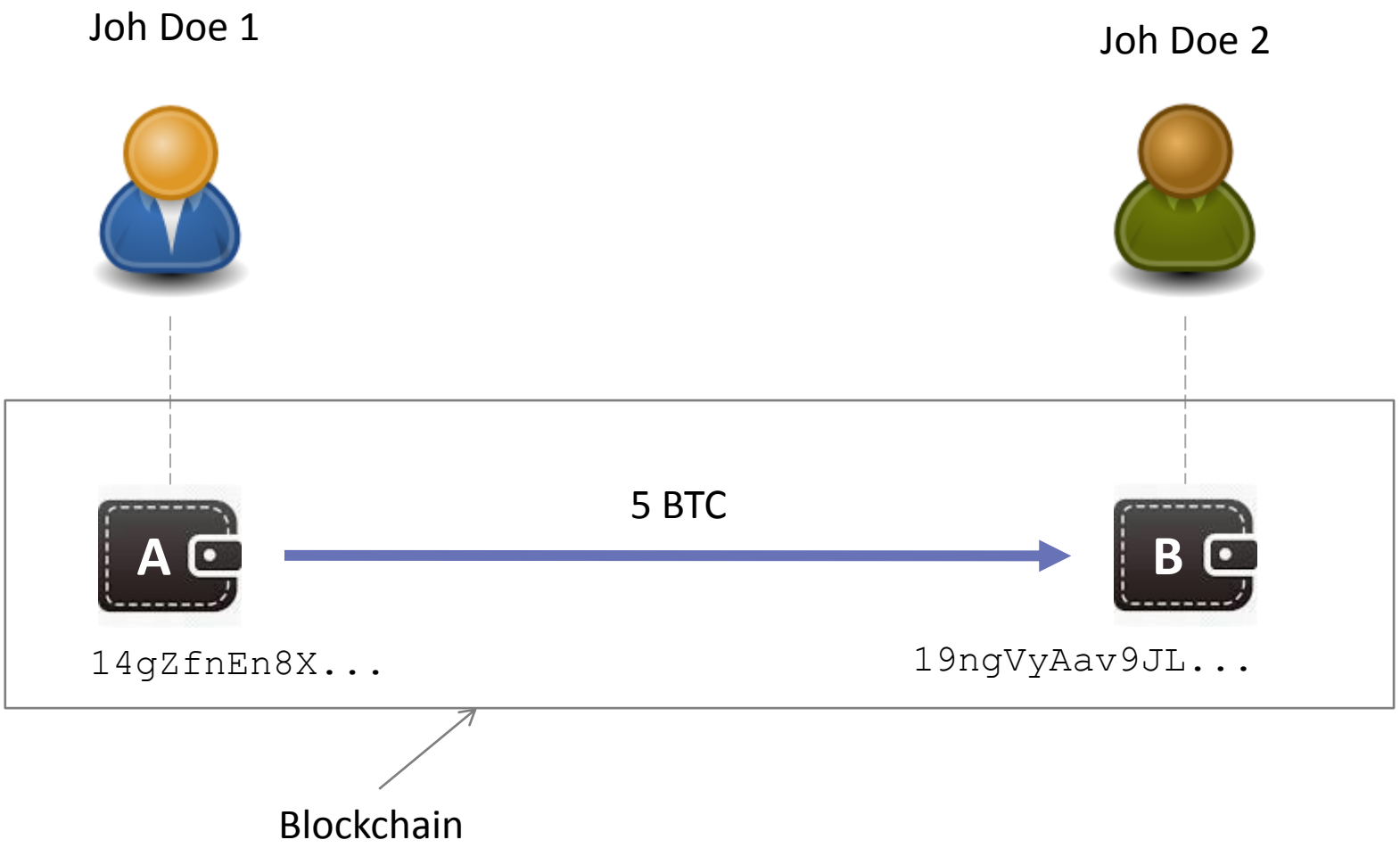


Volatility


1h
12h
1d
1w
1m
3m
1y
All
Jul 18, 2010
to
Jan 24, 2015
$1000
$750
$500
$250
$0
www.coindesk.com
CoinDesk BPI in effect
2011
2012
2013
2014
2015

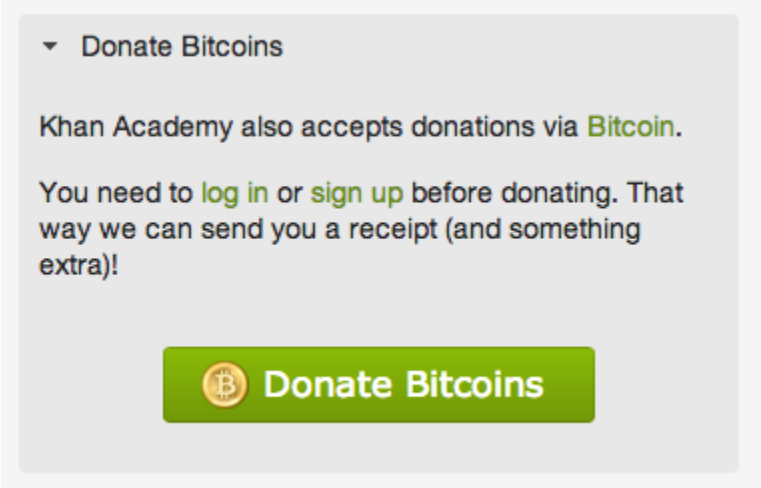
What about security?

Pseudonymity

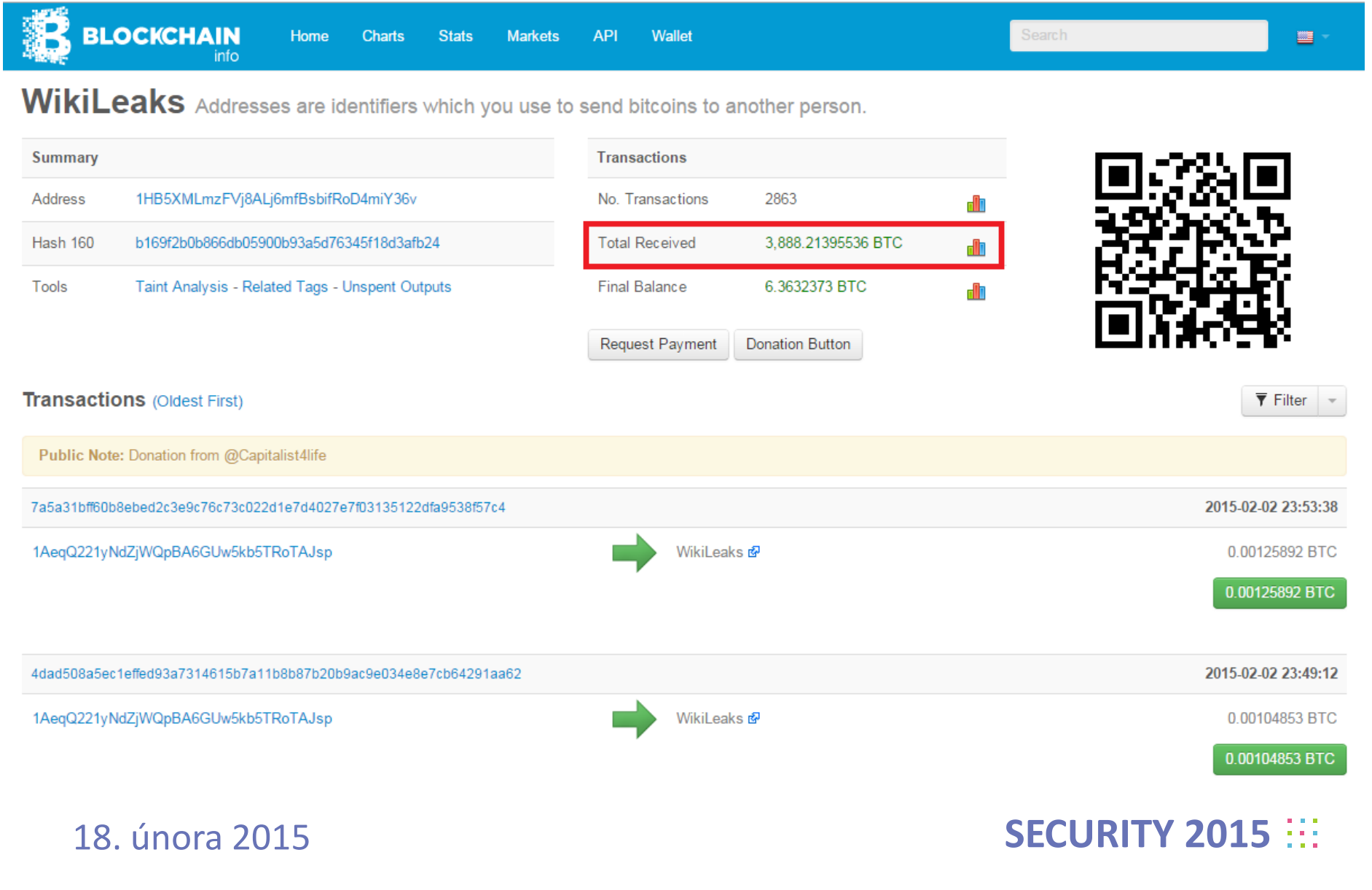


Donate buttons

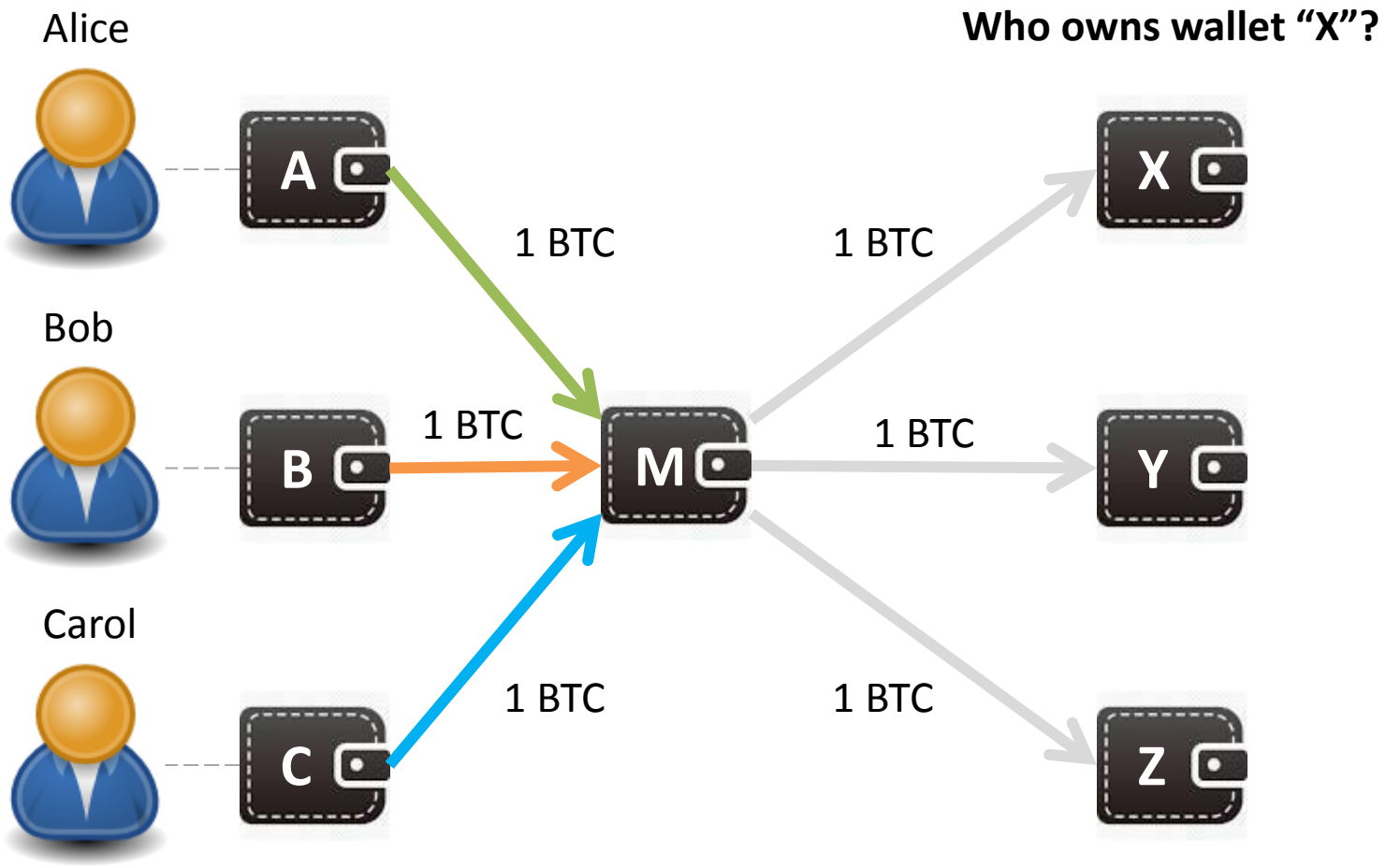
- Reveals **overall sum of donated bitcoins**
- Reveals all **donor's addresses**
- Reveals all **payments from the donation wallet**



Blockchain analysis

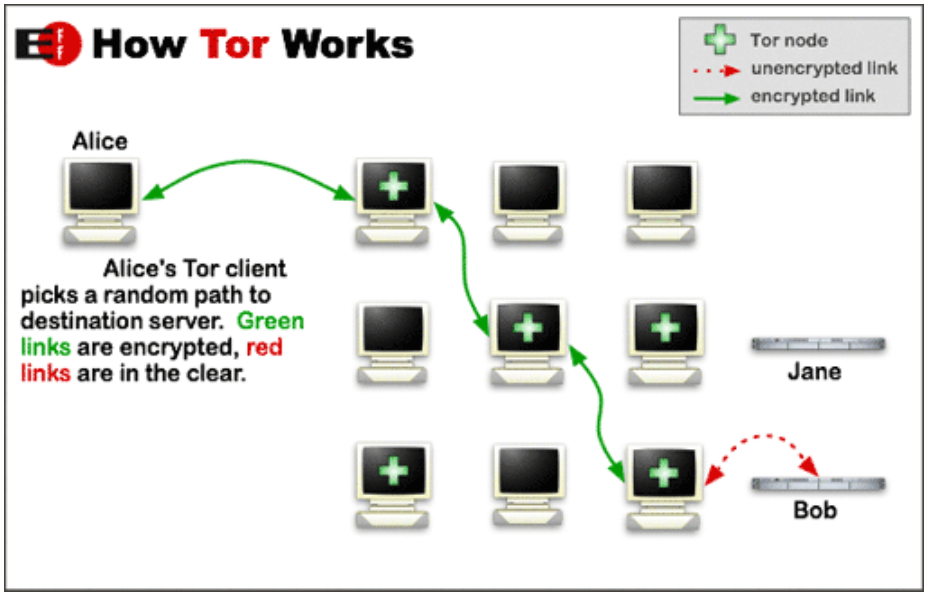


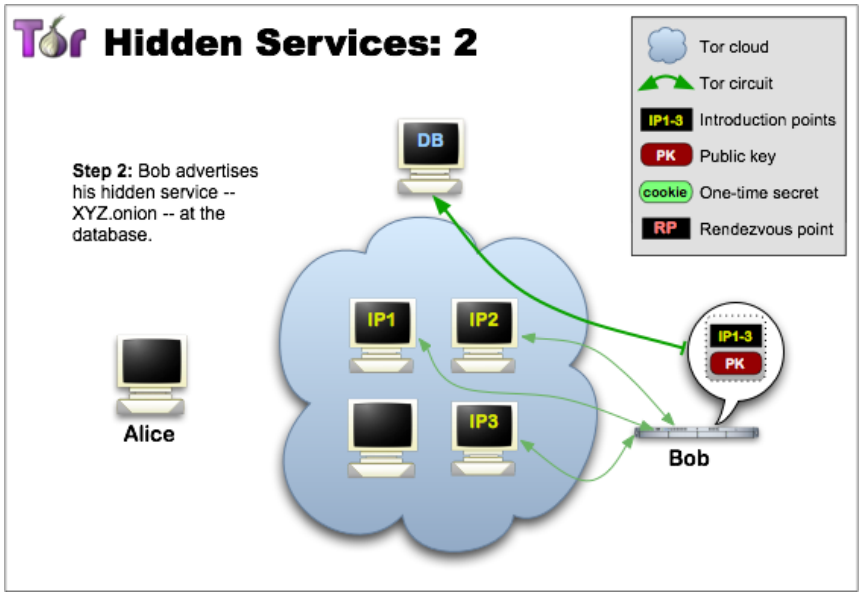
Mixing service



Tor

- The most used **anonymity network**
- Can hide identity of **the client** and **the server**

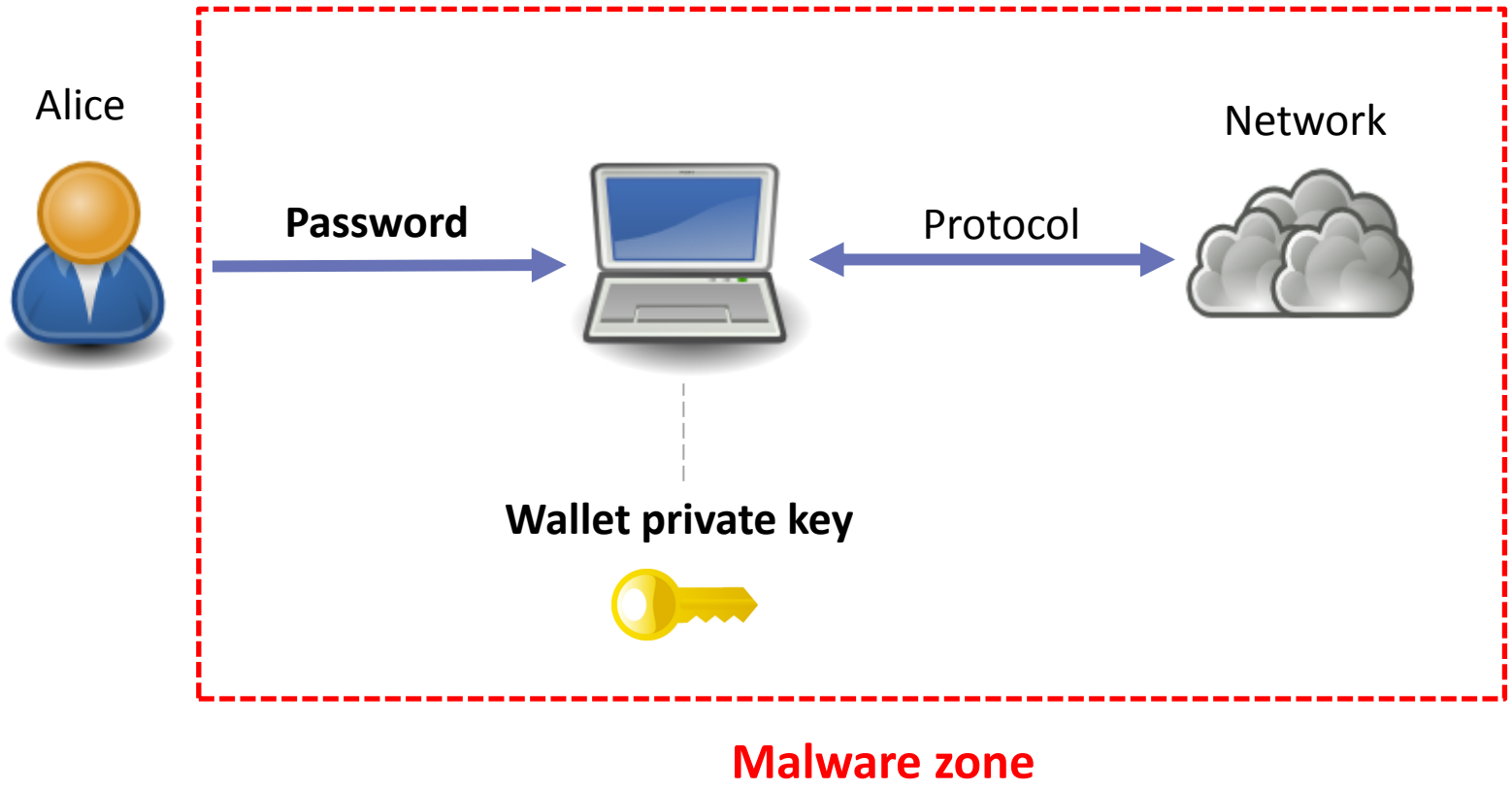




Cryptolocker, CTB Locker ...

- Malware that encrypts HDD and demands **ransom in bitcoins** in exchange for decryption key
- Communicates with C&C server **over Tor**

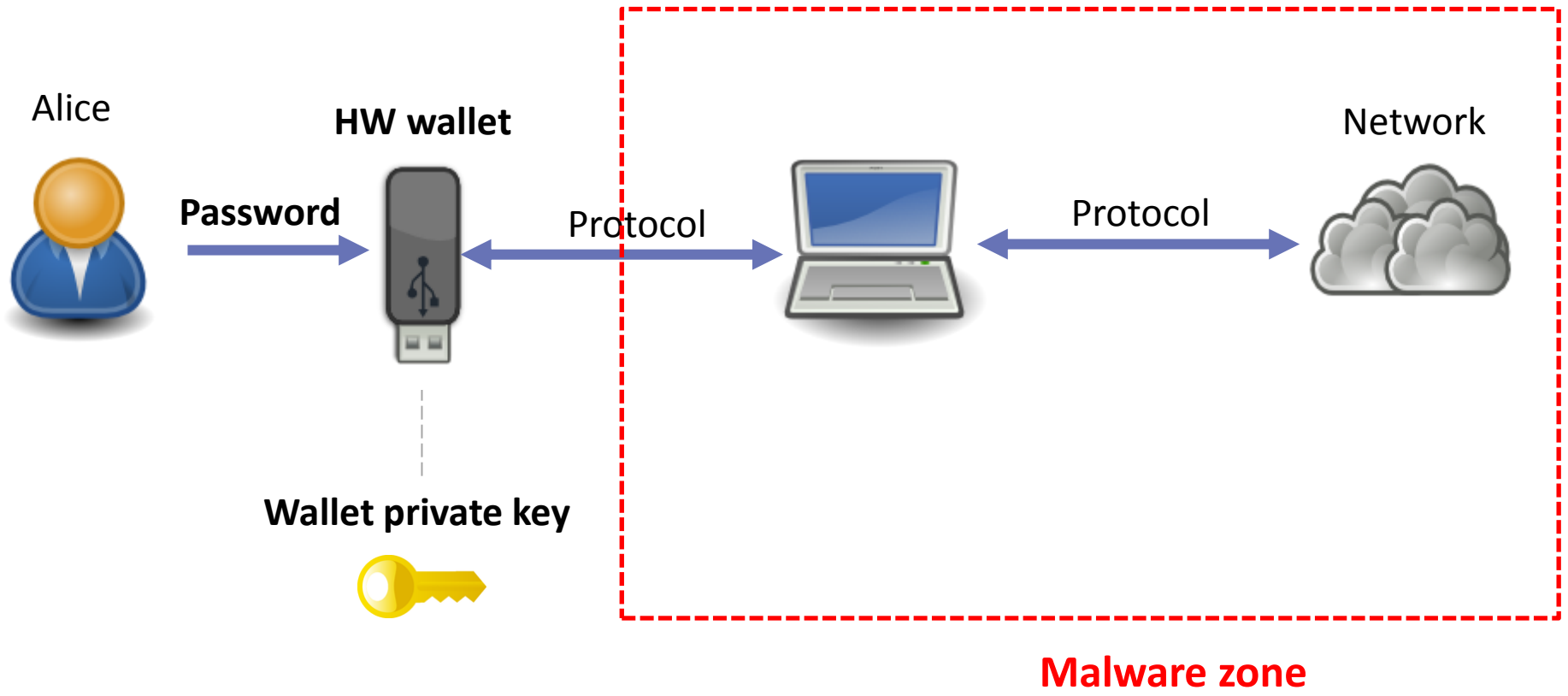
One-factor bitcoin authentication



BadUSB

Video

Two-factor bitcoin authentication



HW wallet

- Private key **never leaves** the HW wallet

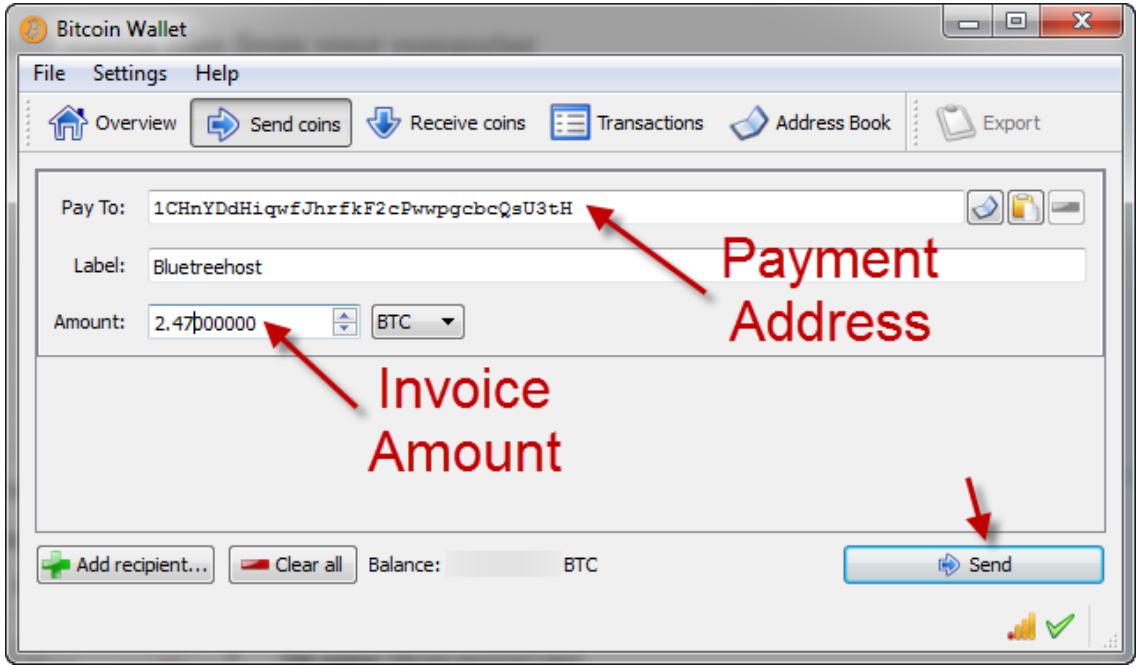
Payment URL

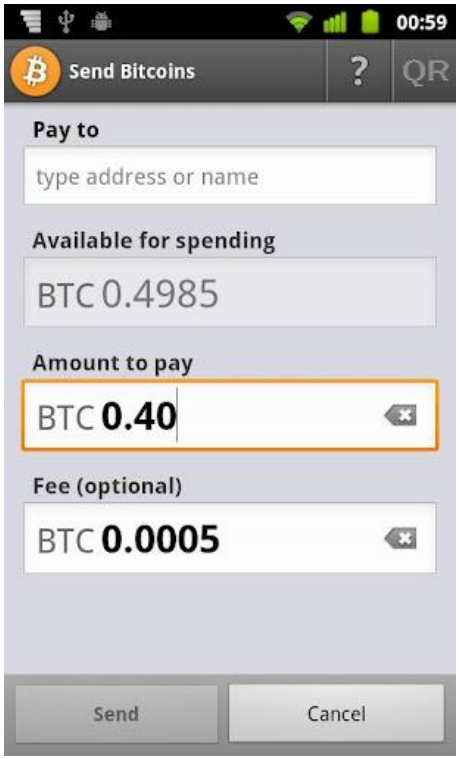
```
payment_address = rpc_call(
        method='getnewaddress',
        params=['eshop']
        )
current_client.order.set_address(payment_address)
client_link = 'bitcoin:' + payment_address + '?amount=' + amount
```

```
<a href="bitcoin:1CHn...3tH?amount=2.47">Pay By Bitcoin</a>
```

Payment URL

- Merchant's address and amount are **not signed**



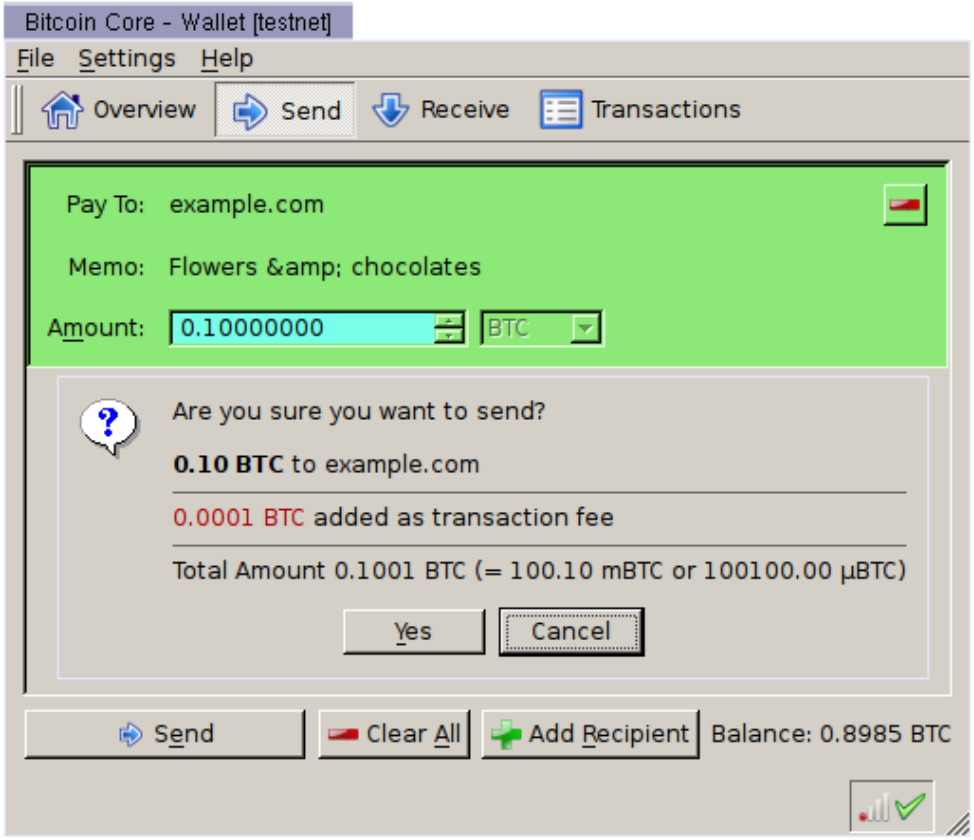


Payment request

```
## Request creation time
details.time = int(time()) ## Current epoch (Unix) time

## Request expiration time
details.expires = int(time()) + 60 * 10 ## 10 minutes from now

## PaymentDetails is complete; serialize it and store it in
PaymentRequest
request.serialized_payment_details = details.SerializeToString()

## Serialized certificate chain
request.pki_data = x509.SerializeToString()

## Initialize signature field so we can sign the full
PaymentRequest
request.signature = ""

## Sign PaymentRequest
request.signature = sign(private_key,
request.SerializeToString(), "sha256")
```

Payment request

- Merchant's address and amount are **signed** by **domain SSL certificate**



Summary

- Advantages
  - **Cheap** international payments
  - **Secure** (does not depend of third party)
  - Very **easy to use** for the merchants and the customers

- Disadvantages
  - **Privacy issues** if used in a wrong way
  - **High volatility** of value
  - **Unsettled legal status** (some use cases lay in gray area)

References

Bitcoin community website
https://bitcoin.org/en/

Mastering Bitcoin (book)
http://chimera.labs.oreilly.com/books/1234000001802/

BadUSB (tools)
https://github.com/adamcaudill/Psychson

CTB locker
http://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information

Tor community website
https://www.torproject.org

Handbook of Peer-to-Peer Networking (book)
http://www.springer.com/gp/book/9780387097503

SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Ing. Adam Brunai

AEC, spol. s r.o.

adam.brunai@aec.cz