Lykke

Blockchain Settlement: Protocols and Scalability Issues

Michael Nikulin

2016

Agenda

I. What is Bitcoin

II. Blockchain. How does it work?

III. Cryptoassets

IV. Blockchain Scalability Issues

Bitcoin

Bitcoin is the first decentralized cryptocurrency

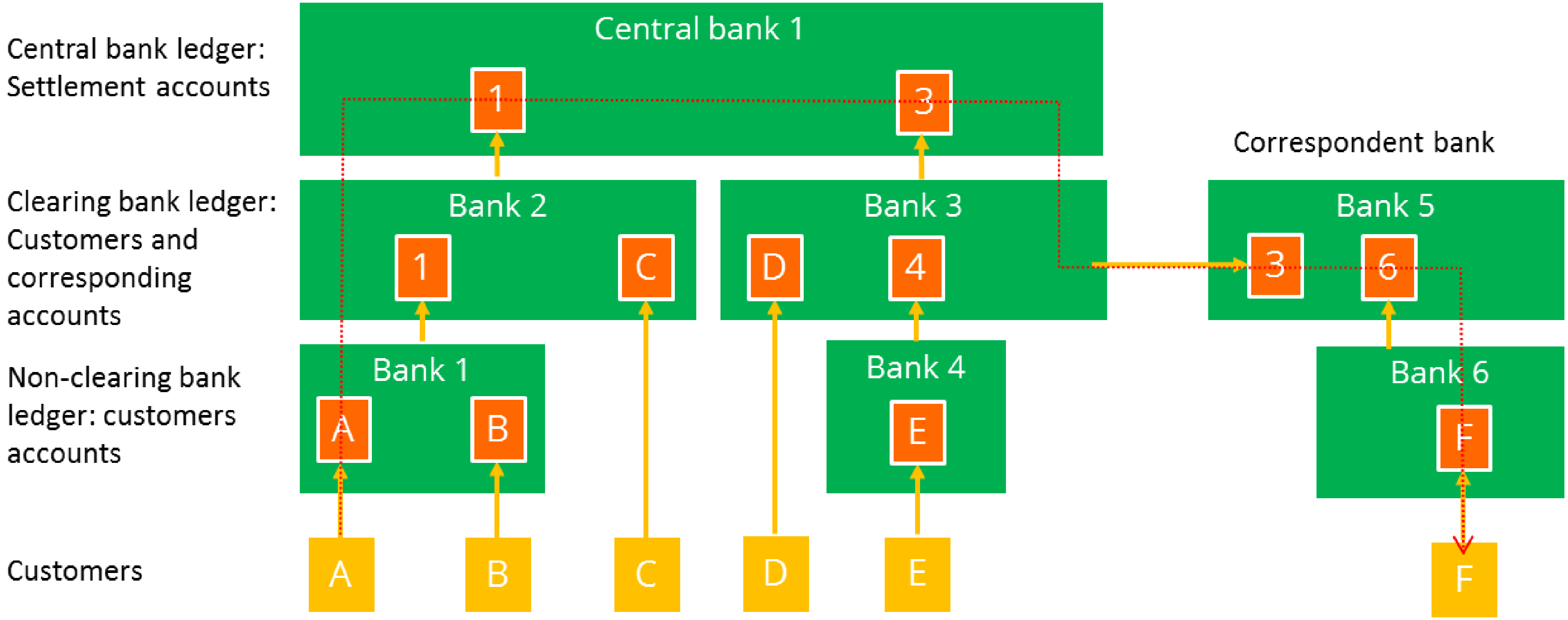
Bitcoin Forks

- Litecoin
- Namecoin
- PPCoin, Novacoin (Proof Of Stake)
- Terracoin
- Chinacoin
- Rucoin
- Ripple (not a Bitcoin fork)
- etc.

Why Bitcoin?

Peer-to-peer electronic payment system

Why do we need all these middlemen?



Central bank ledger: Settlement accounts

Clearing bank ledger: Customers and corresponding accounts

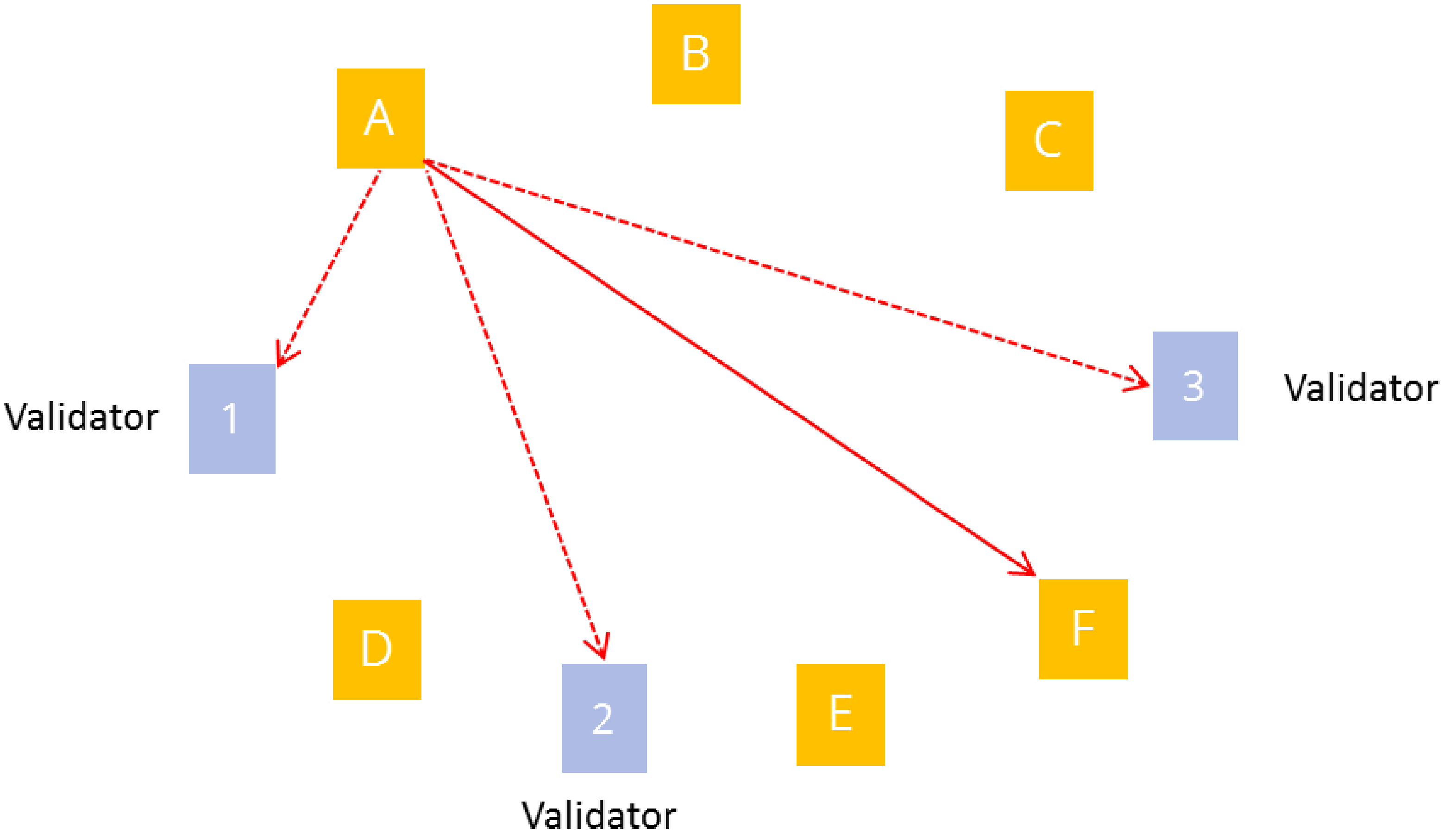
Non-clearing bank ledger: customers accounts

Customers

Correspondent bank

Traditional payment system

Why do we need all these middlemen?



Decentralized payment system

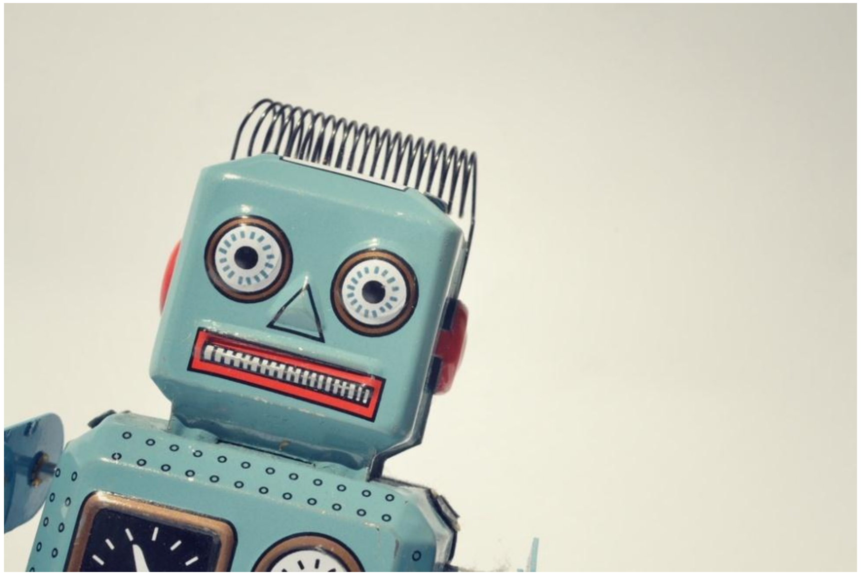
Because Of The Information Nature

Data copy restriction is really tough thing

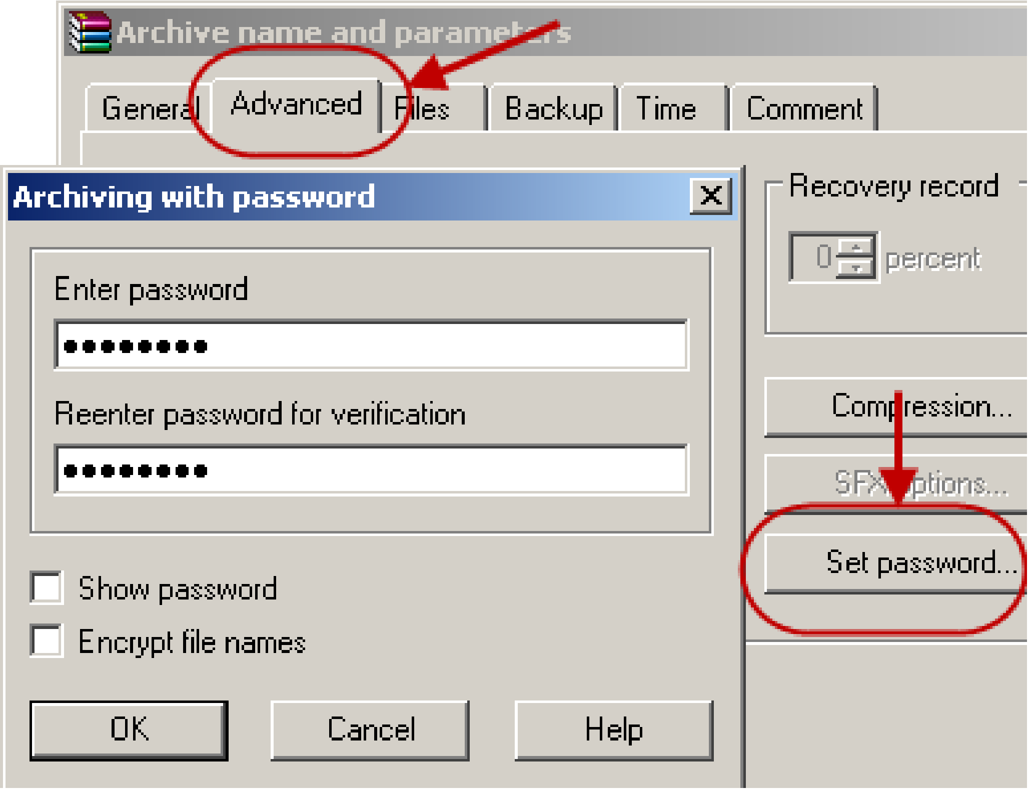
What Means “Crypto”?

Cryptocurrency is based on

Asymmetric Signatures Algorithms



Symmetric Encryption



Archive name and parameters

Archiving with password

Enter password

●●●●●●●●●

Reenter password for verification

●●●●●●●●●

□ Show password

□ Encrypt file names

Asymmetric signatures algorithms

I owe you $10 000

Public key – e-mail address

akFHMX1KJGbCN1niSXFu6MKv7KCrezKDRVn

Private key – password

L4FHDBRN6Egz4kch3GZBcEoAucQGX2iBci4Ld7iNXjQ7V8fjkMH4

Lykke Asymmetric signatures algorithms

I owe you $10 000

Is it a cryptocurrency?

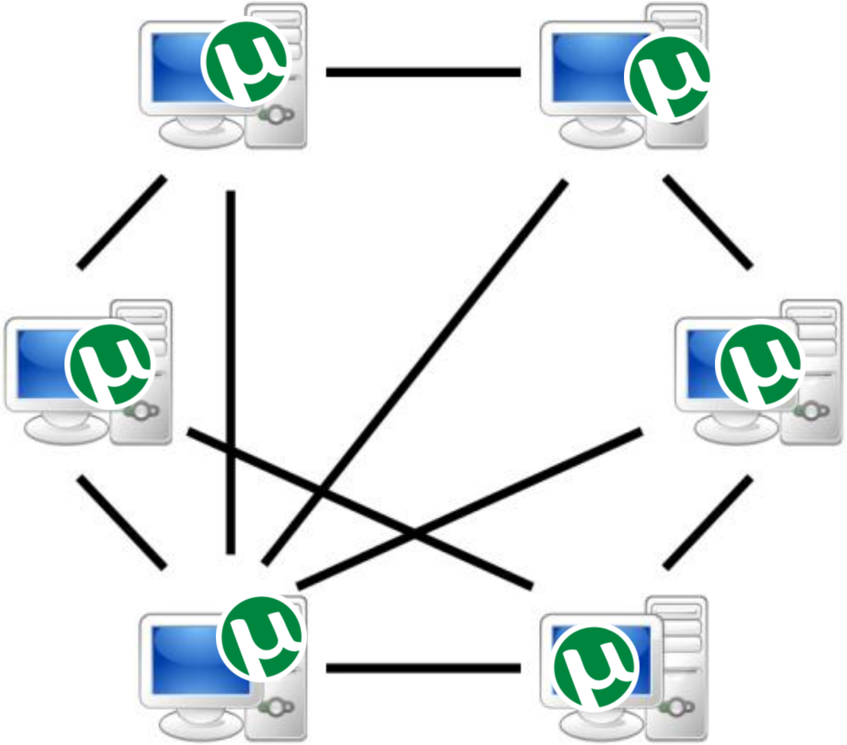
Public key – e-mail address

akFHMX1KJGbCN1niSXFu6MKv7KCrezKDRVn

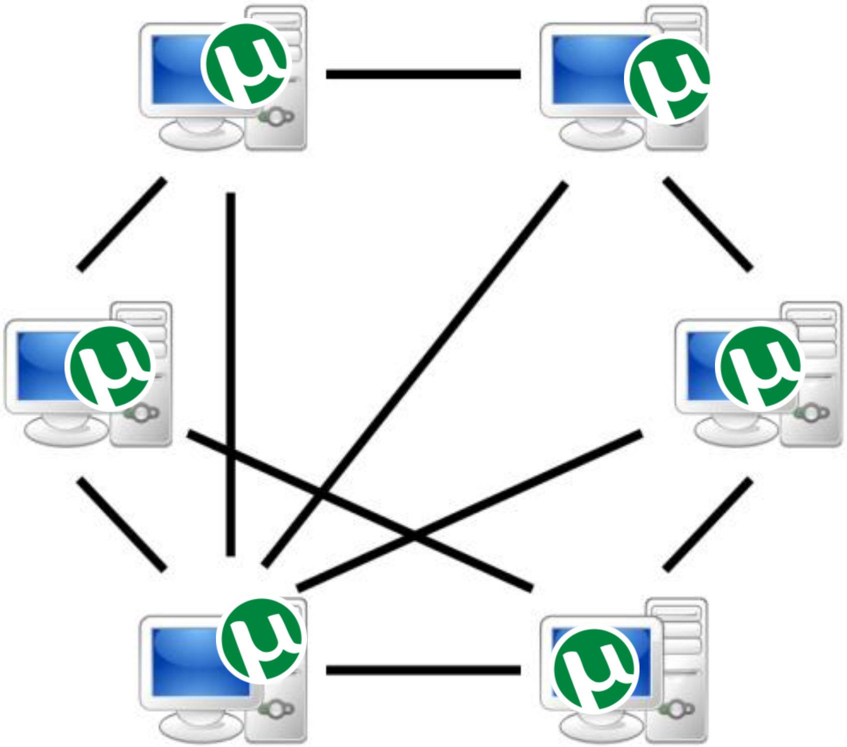
Private key – password

L4FHDBRN6Egz4kch3GZBcEoAucQGX2iBci4Ld7iNXjQ7V8fjkMH4

Distributed Ledger

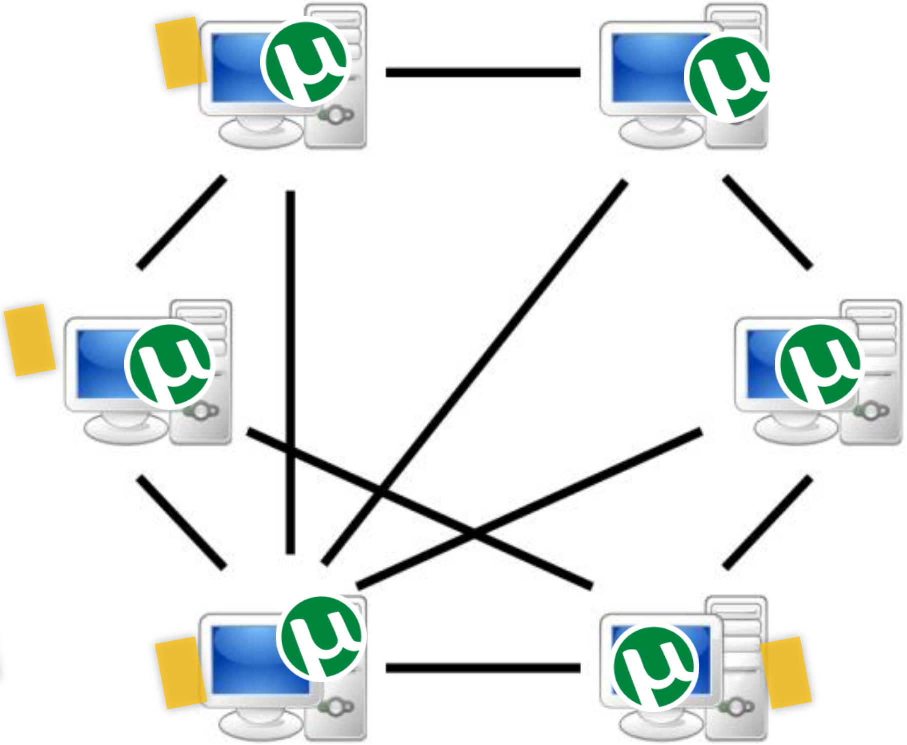


How To Update Distributed Ledger



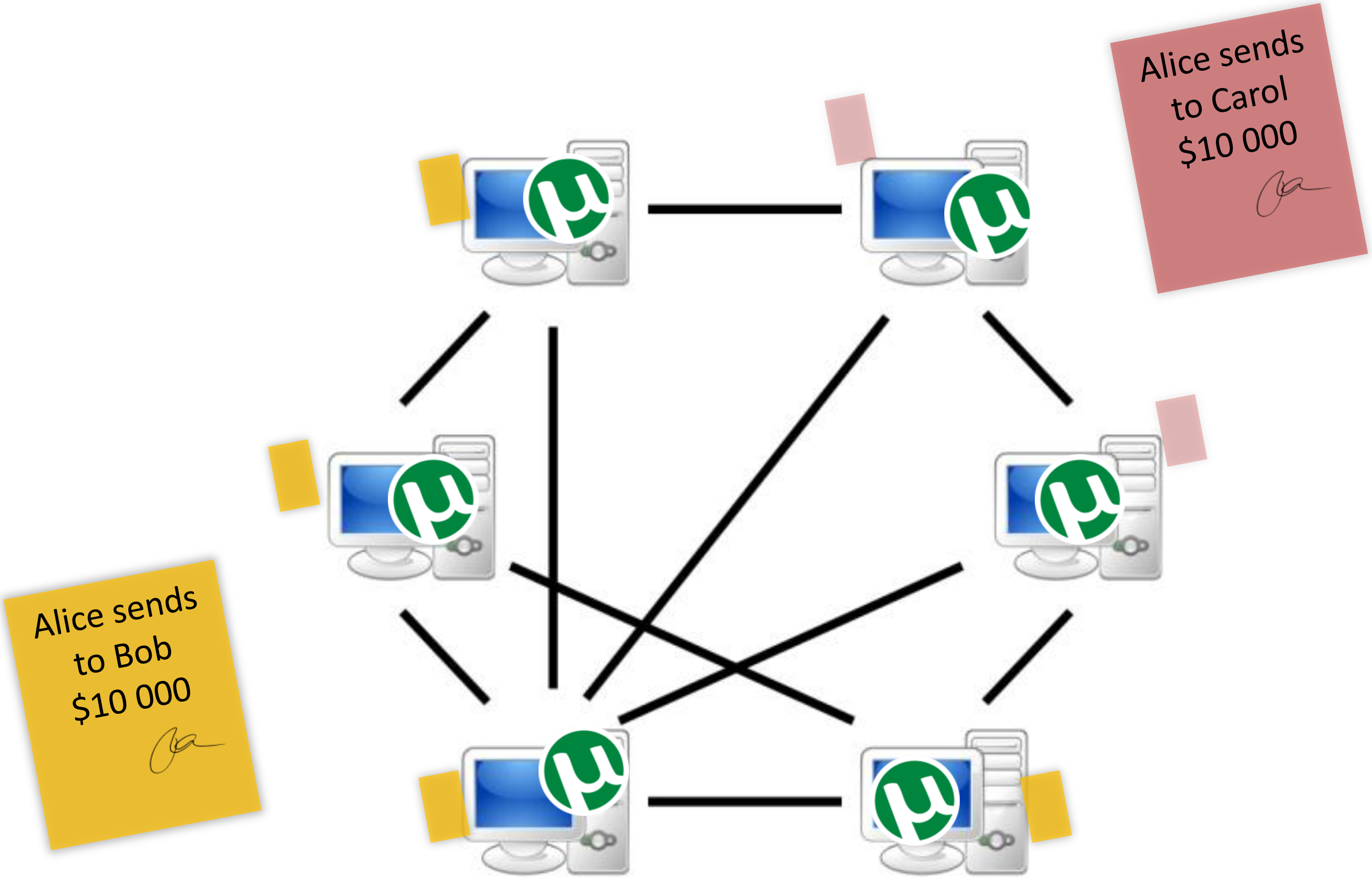
Alice sends
to Bob
$10 000

How To Update Distributed Ledger



Alice sends
to Bob
$10 000

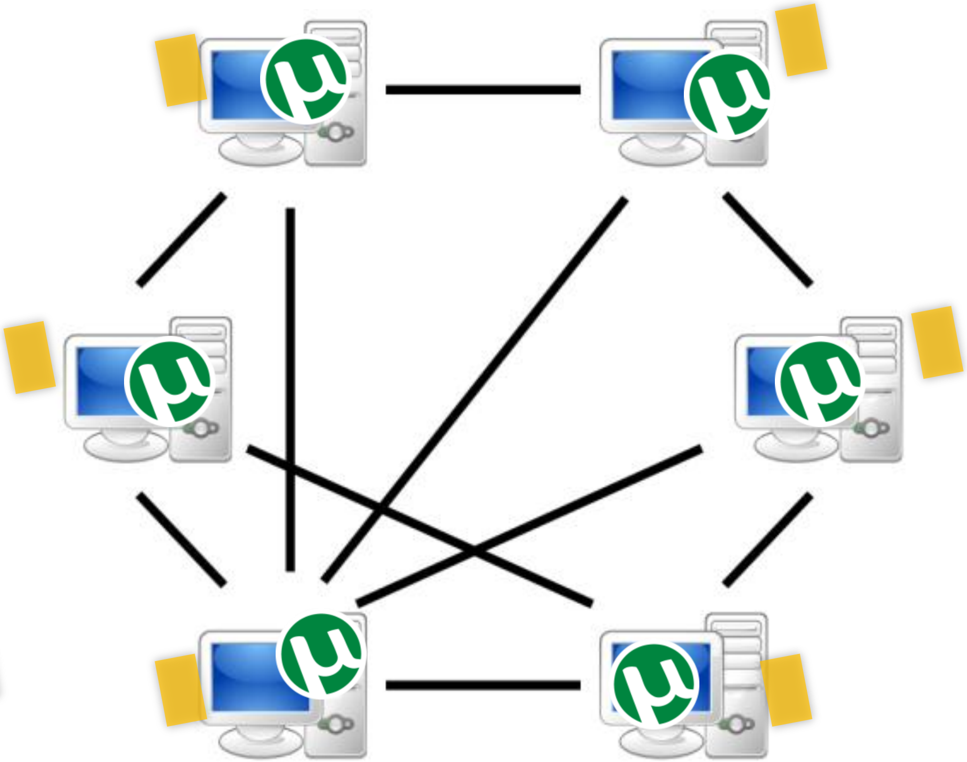
Double-Spending Attack



Alice sends to Carol $10 000

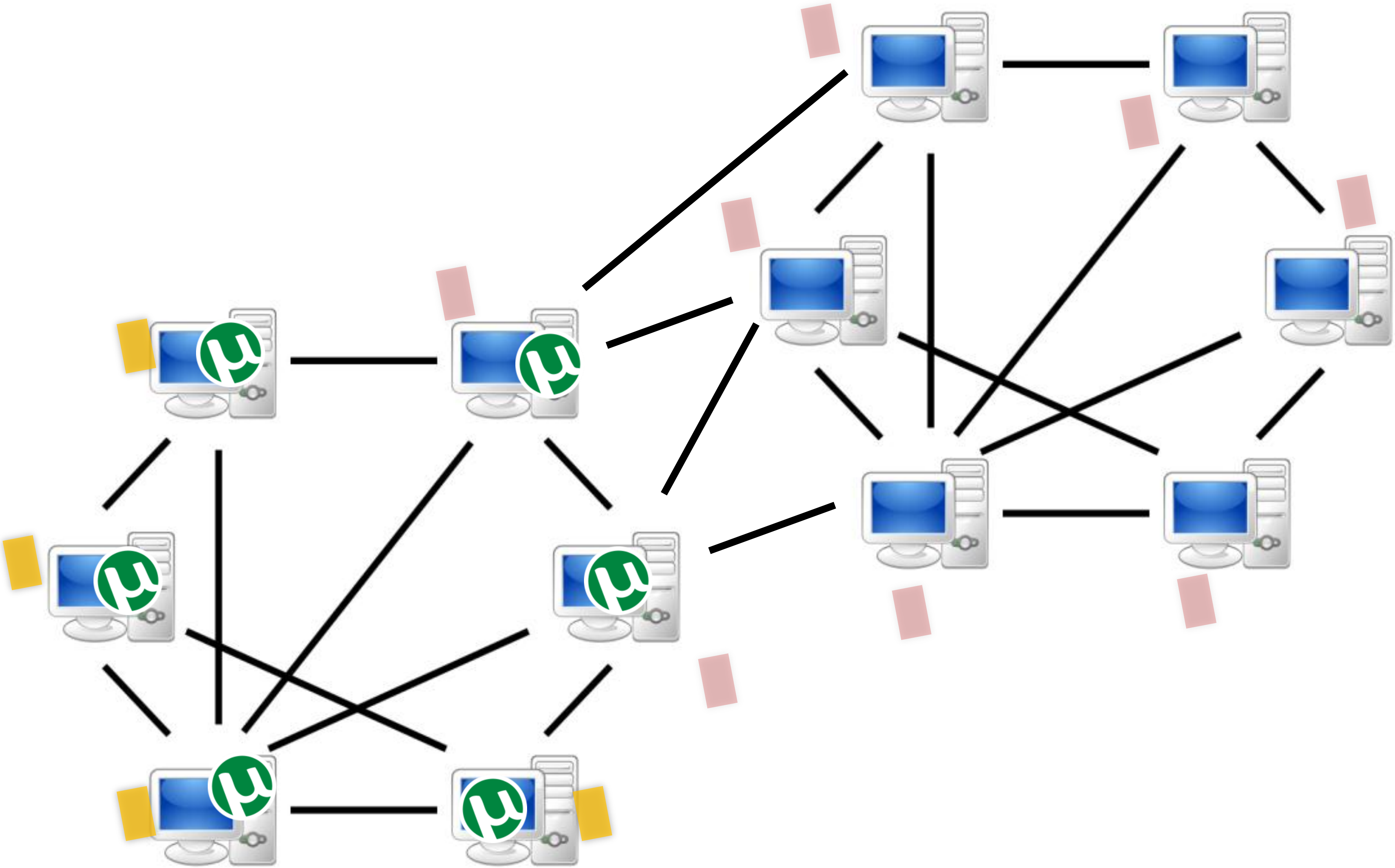
Alice sends to Bob $10 000

Protection of Double-Spending



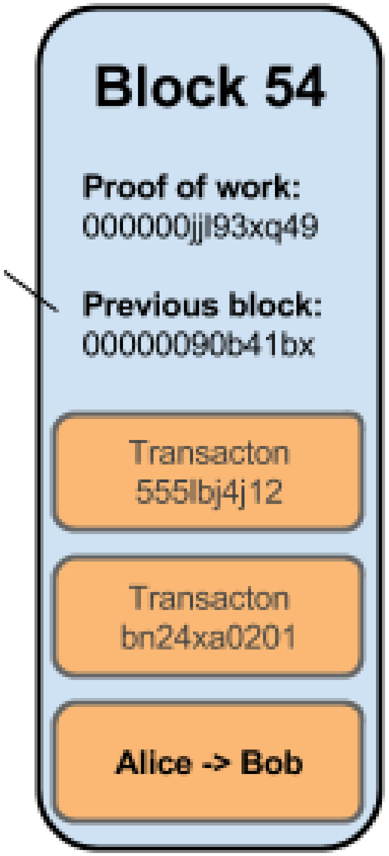
Alice sends
to Bob
$10 000

Majority Attack



Proof-of-work

The ‘work’ must be a task that is hard for a computer to complete, but easy for other computers to verify.



Block 54

Proof of work:
000000jjl93xq49

Previous block:
00000090b41bx

Transacton
555lbj4j12

Transacton
bn24xa0201

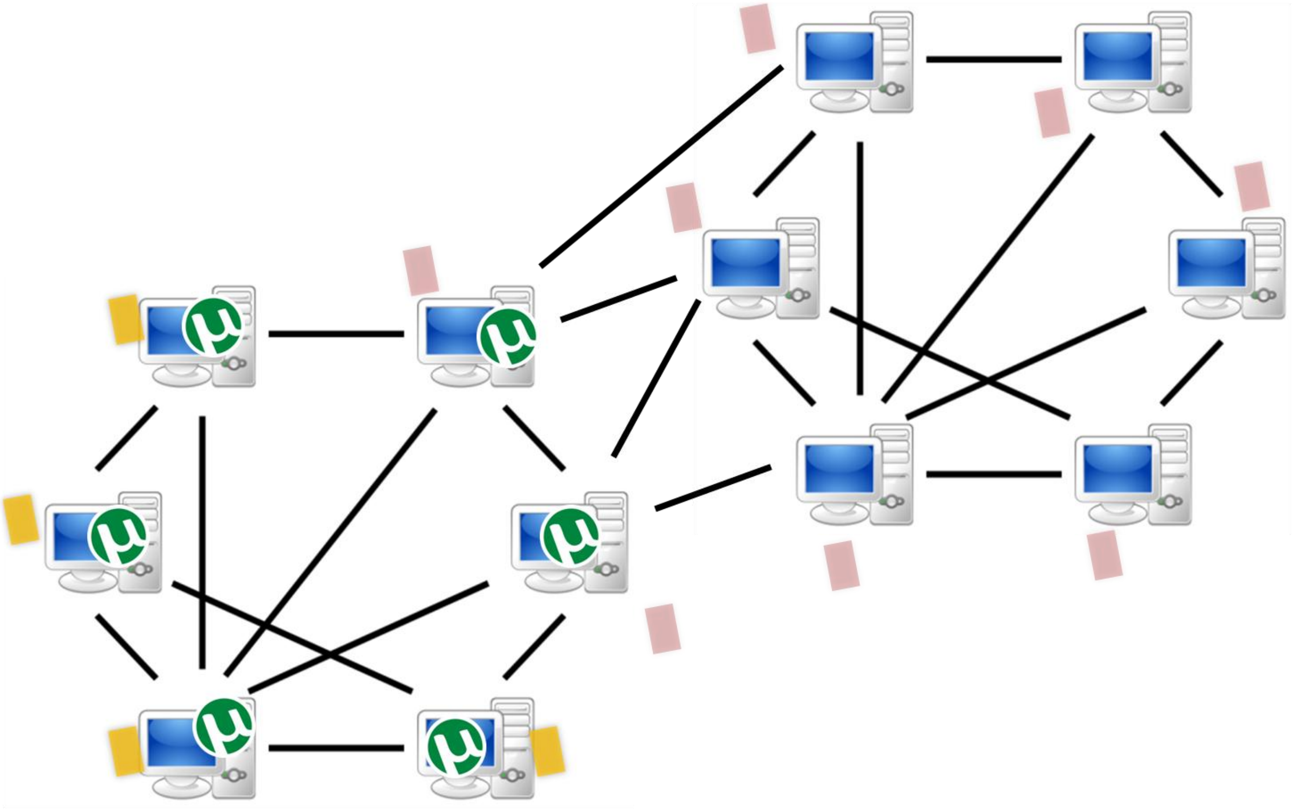
Alice -> Bob

A simple example would be a requirement that people repeatedly roll three six-sided dice until they roll three ones.

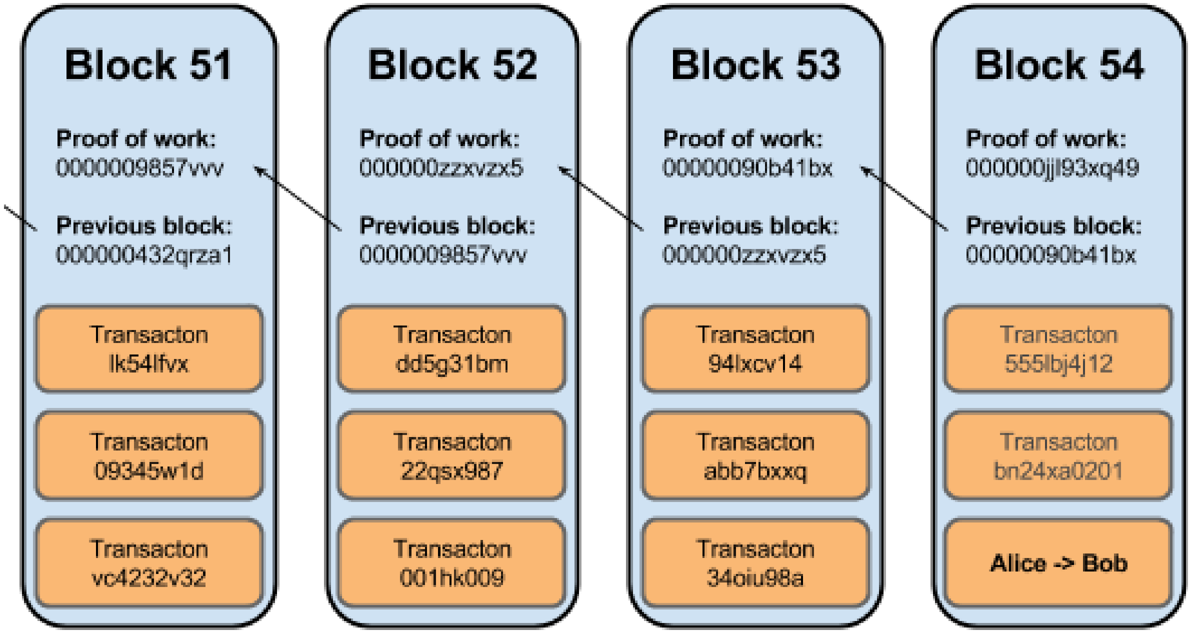
Difficulty of the work recalculated every 2016 blocks. Rate of block generation targeting 1 new block in 10 minutes

Majority Attack

Majority attack requires >51% of Bitcoin network power ($300 mln)



Chain of blocks



Block 51

Proof of work:
0000009857vvv

Previous block:
000000432qrza1

Transacton
lk54lfvx

Transacton
09345w1d

Transacton
vc4232v32

Block 52

Proof of work:
000000zzxvzx5

Previous block:
0000009857vvv

Transacton
dd5g31bm

Transacton
22qsx987

Transacton
001hk009

Block 53

Proof of work:
00000090b41bx

Previous block:
000000zzxvzx5

Transacton
94lxcv14

Transacton
abb7bxxq

Transacton
34oiu98a

Block 54

Proof of work:
000000jjl93xq49

Previous block:
00000090b41bx

Transacton
555lbj4j12

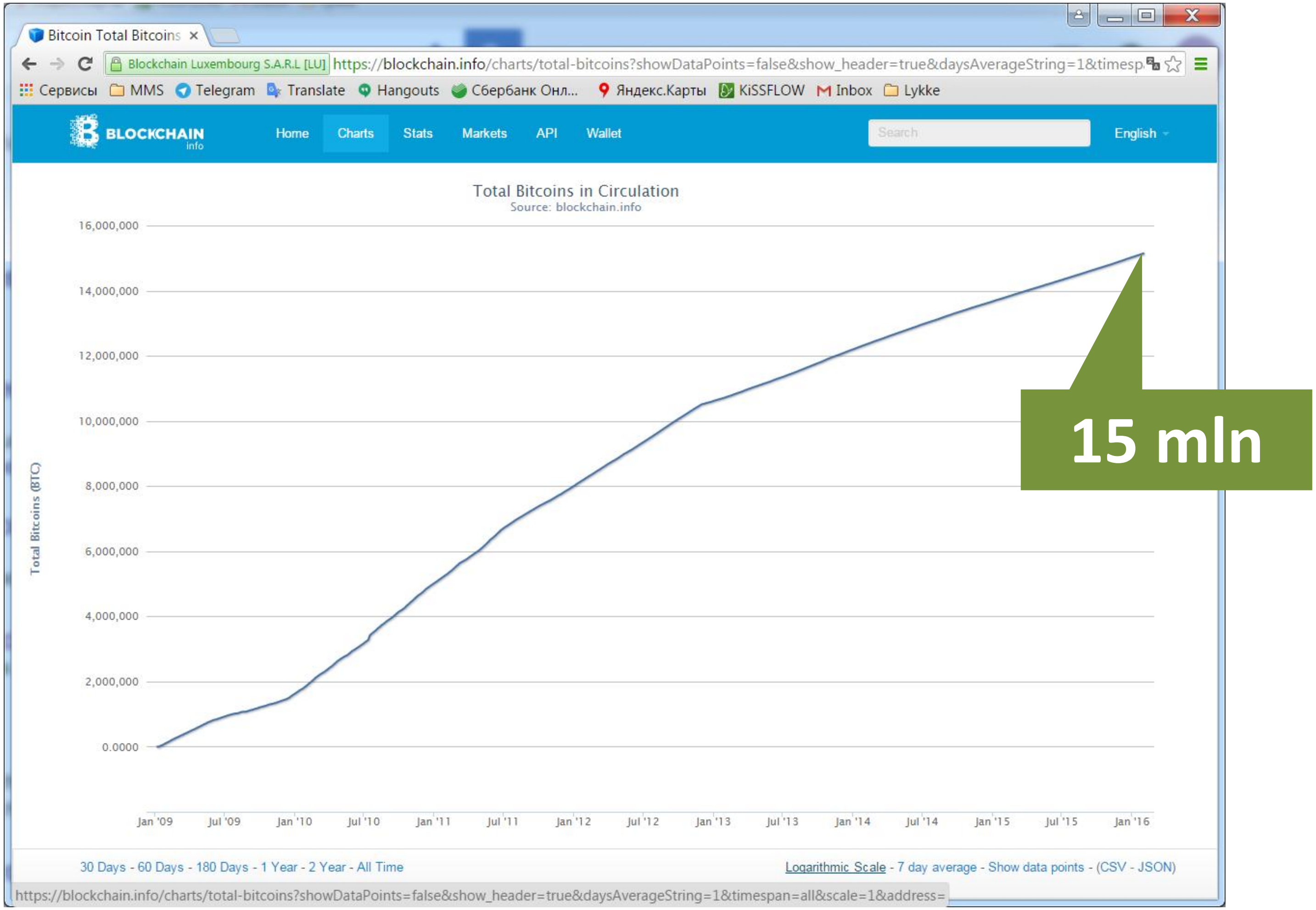
Transacton
bn24xa0201

Alice -> Bob

- Miner is awarded the fees paid by users sending transactions
- When a new block is discovered, the miner may award themselves a certain number of bitcoins (~25BTC)

Lykke

Bitcoins In Circulation



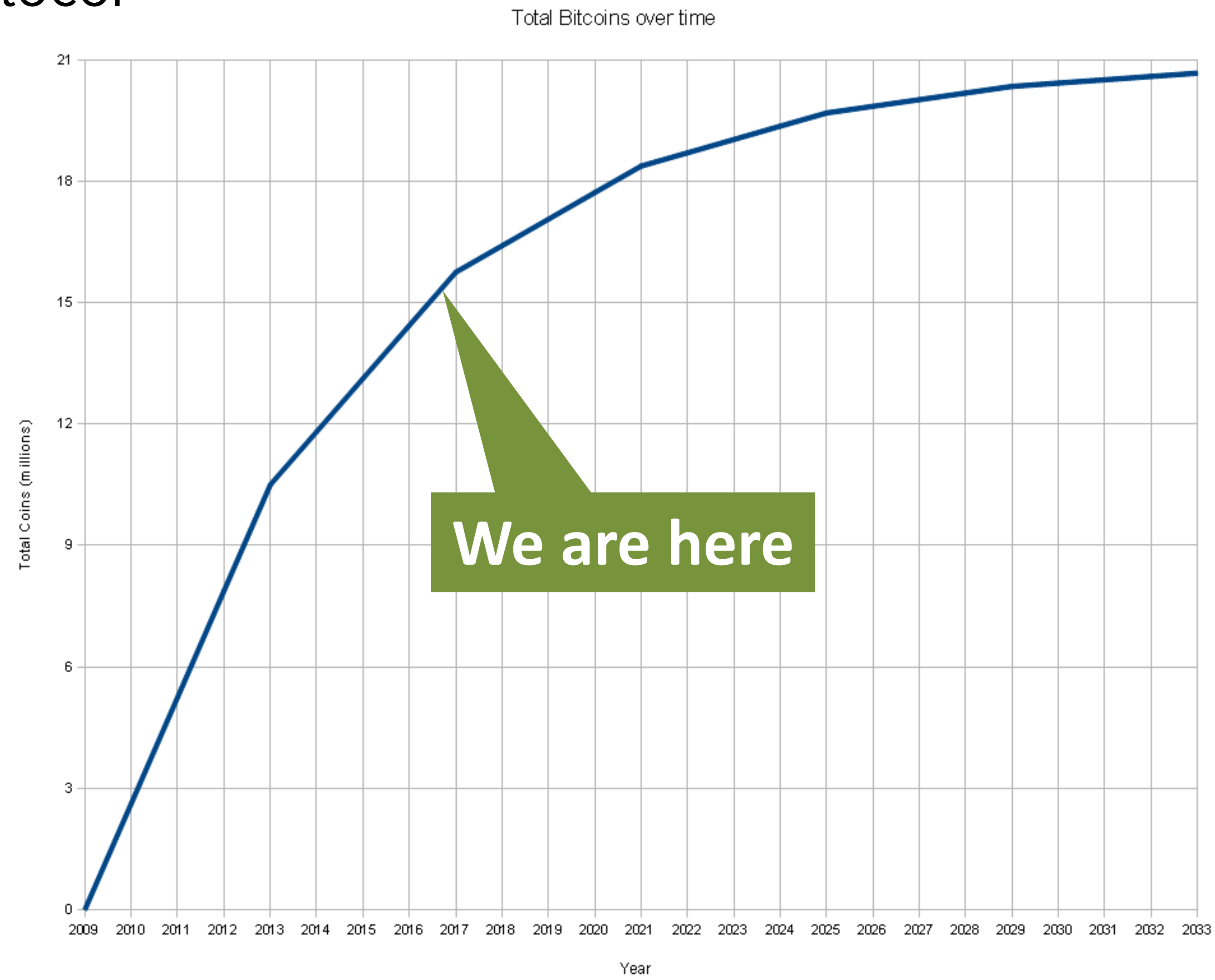
Bitcoin Total Bitcoins ×
Blockchain Luxembourg S.A.R.L [LU] https://blockchain.info/charts/total-bitcoins?showDataPoints=false&show_header=true&daysAverageString=1&timesp
Сервисы
MMS
Telegram
Translate
Hangouts
Сбербанк Онл...
Яндекс.Карты
KiSSFLOW
Inbox
Lykke
BLOCKCHAIN info
Home
Charts
Stats
Markets
API
Wallet
Search
English
Total Bitcoins in Circulation
Source: blockchain.info
Total Bitcoins (BTC)
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
0.0000
Jan '09
Jul '09
Jan '10
Jul '10
Jan '11
Jul '11
Jan '12
Jul '12
Jan '13
Jul '13
Jan '14
Jul '14
Jan '15
Jul '15
Jan '16
30 Days - 60 Days - 180 Days - 1 Year - 2 Year - All Time
Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)
https://blockchain.info/charts/total-bitcoins?showDataPoints=false&show_header=true&daysAverageString=1&timespan=all&scale=1&address=

15 mln

Mined Bitcoins introduce into the system

Bitcoin Miners

The limit of 21 million bitcoins is "hard-wired" in to the protocol

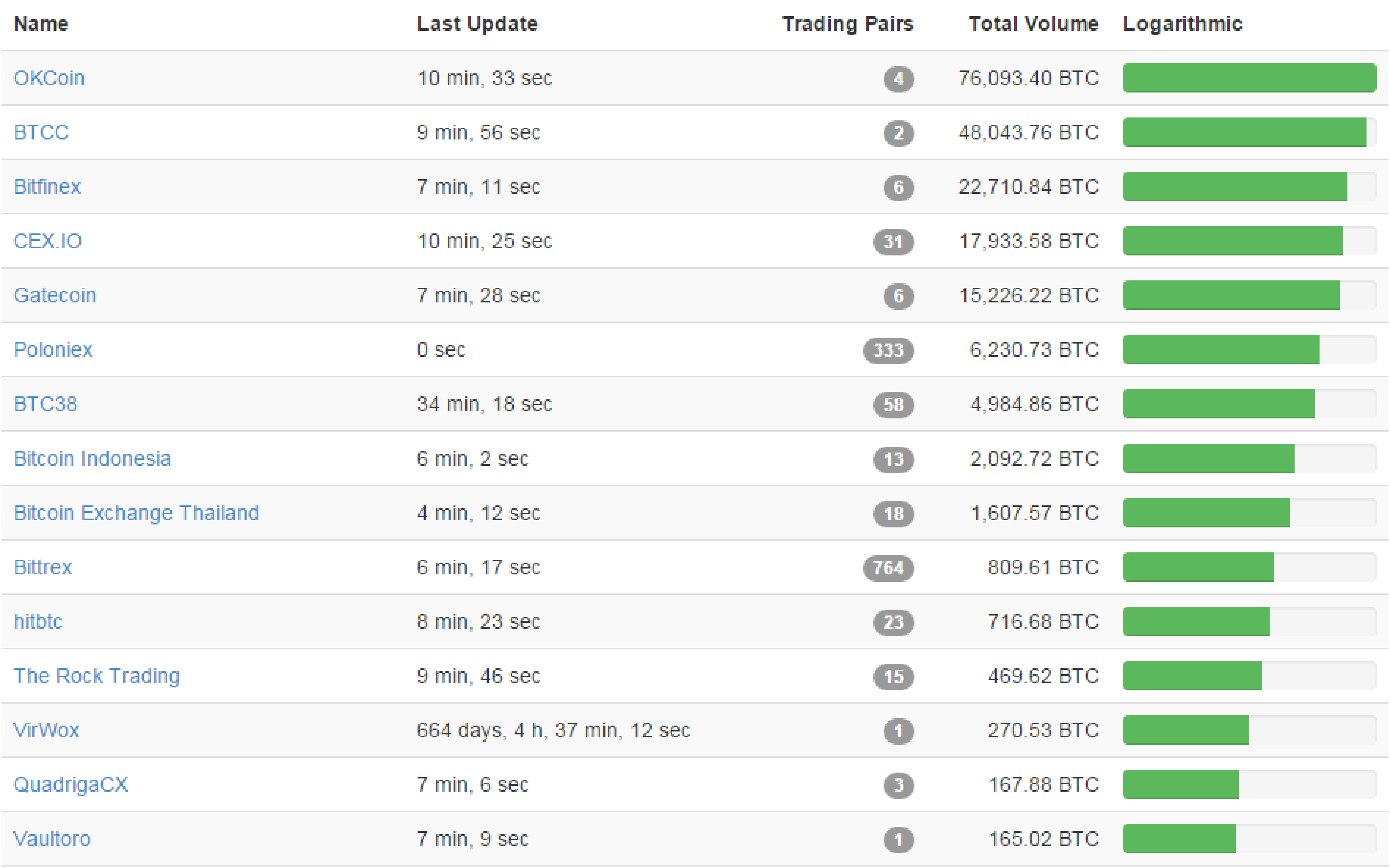


Satoshi Nakamoto

- Cryptocurrency history can be traced back to DigiCash started David Chaum in 1990’s
- Oct 31, 2008 Satoshi Nakamoto publishes white paper titled Bitcoin: A Peer-to-Peer Electronic Cash System via “The Cryptography Mailing List”. This innovation draws on advances from a range of disciplines including cryptography (secure communication), game theory (strategic decision-making) and peer-to-peer networking (networks of connections formed without central co-ordination)
- Jan 3, 2009 Satoshi releases Bitcoin source code and software client to the world.

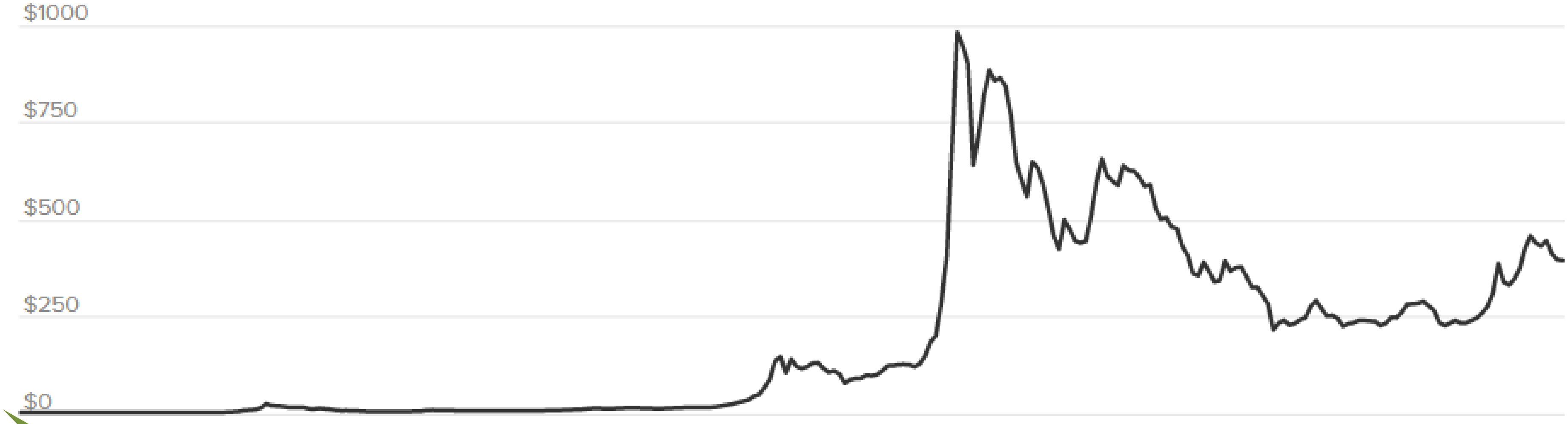
Lykke

Cryptocurrency Exchanges



Name	Last Update	Trading Pairs	Total Volume	Logarithmic
OKCoin	10 min, 33 sec	4	76,093.40 BTC	🟩
BTCC	9 min, 56 sec	2	48,043.76 BTC	🟩
Bitfinex	7 min, 11 sec	6	22,710.84 BTC	🟩
CEX.IO	10 min, 25 sec	31	17,933.58 BTC	🟩
Gatecoin	7 min, 28 sec	6	15,226.22 BTC	🟩
Poloniex	0 sec	333	6,230.73 BTC	🟩
BTC38	34 min, 18 sec	58	4,984.86 BTC	🟩
Bitcoin Indonesia	6 min, 2 sec	13	2,092.72 BTC	🟩
Bitcoin Exchange Thailand	4 min, 12 sec	18	1,607.57 BTC	🟩
Bittrex	6 min, 17 sec	764	809.61 BTC	🟩
hitbtc	8 min, 23 sec	23	716.68 BTC	🟩
The Rock Trading	9 min, 46 sec	15	469.62 BTC	🟩
VirWox	664 days, 4 h, 37 min, 12 sec	1	270.53 BTC	🟩
QuadrigaCX	7 min, 6 sec	3	167.88 BTC	🟩
Vaultoro	7 min, 9 sec	1	165.02 BTC	🟩

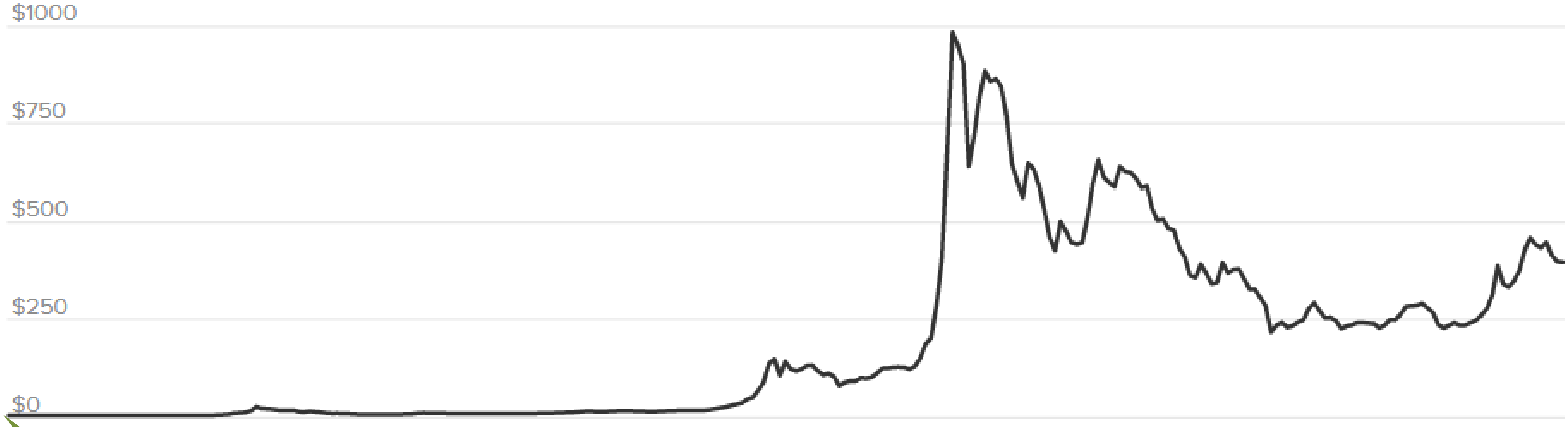
Bitcoin Price, USD



$0.008

May of 2010

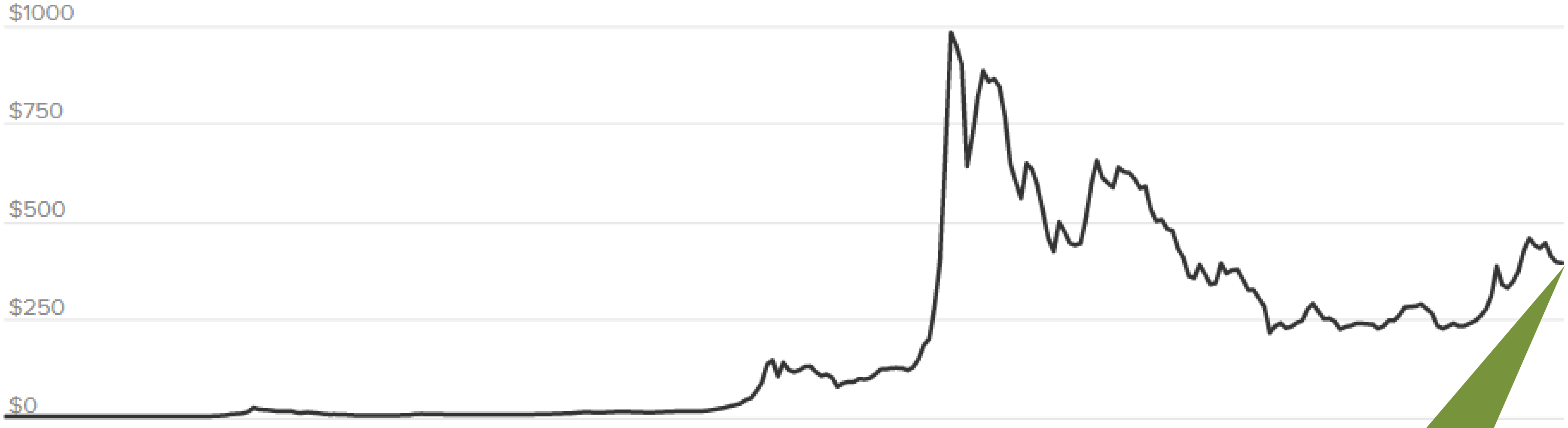
Bitcoin Price, USD



22nd May 2010 Bitcoin Pizza Day

Bought on 22nd May 2010 by Laszlo Hanyecz, the programmer paid a fellow Bitcoin Talk forum user 10,000 BTC for two Papa John’s pizzas ($25)

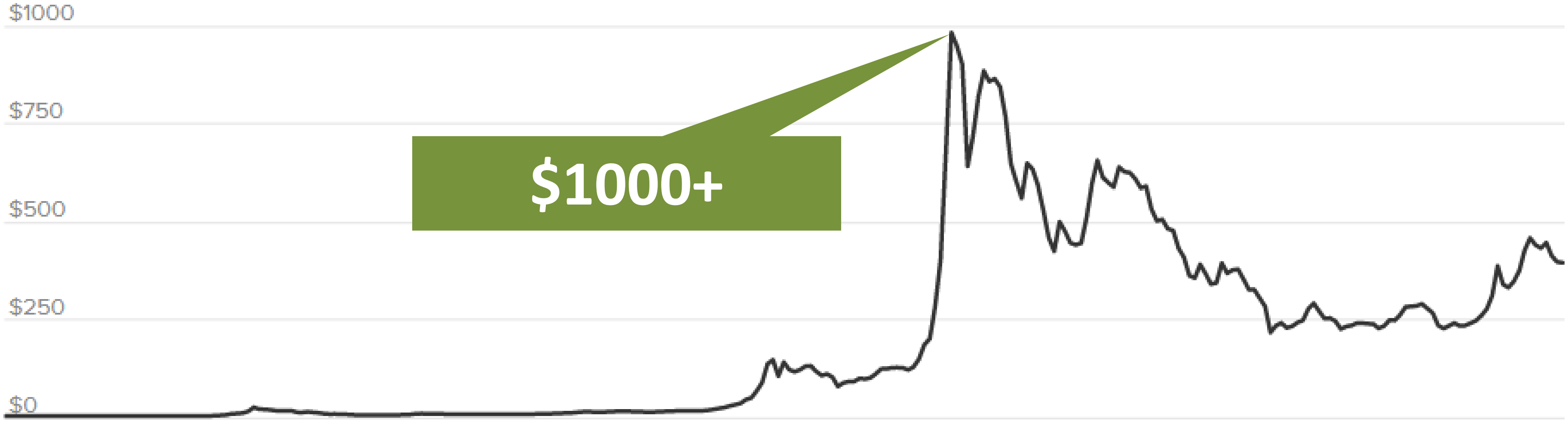
Bitcoin Price, USD



$392.19

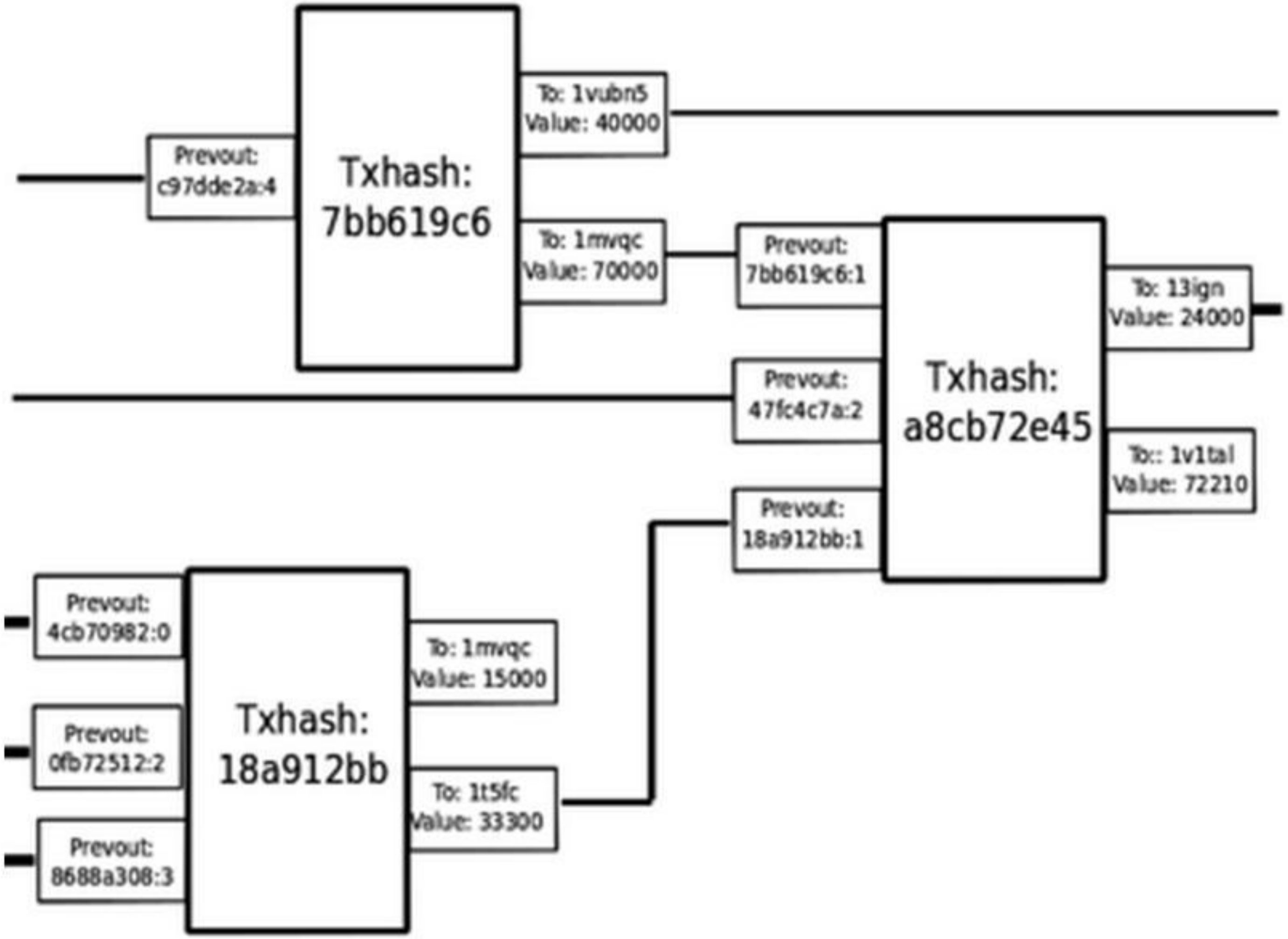
25.01.2015

Bitcoin Price, USD



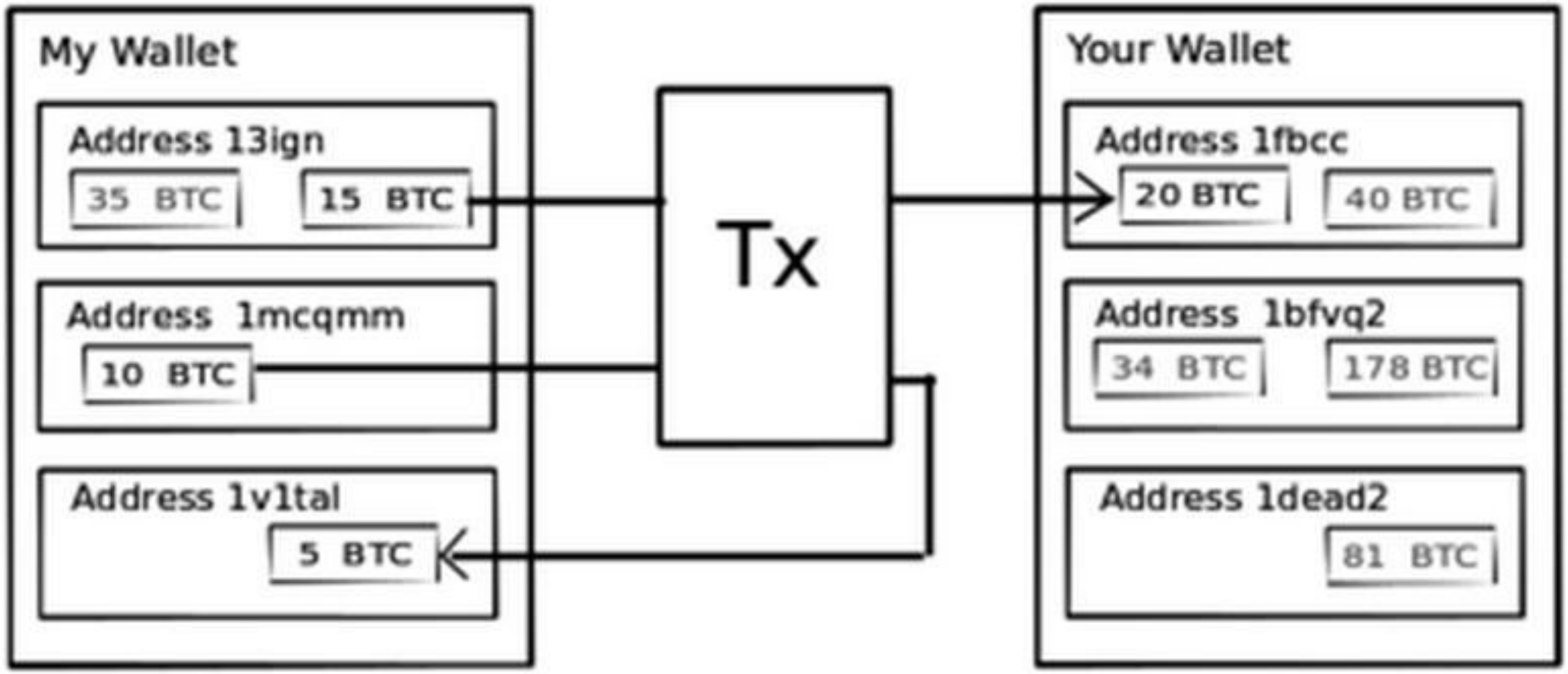
$1000+

Bitcoin Transactions



There is no notion “balance” on blockchain

Blockchain Transactions



Change on blockchain

Cryptoassets

Criptoassets

Satoshi – is the smallest fraction of a Bitcoin that can currently be sent

100 000 000 Satoshi = 1 BTC

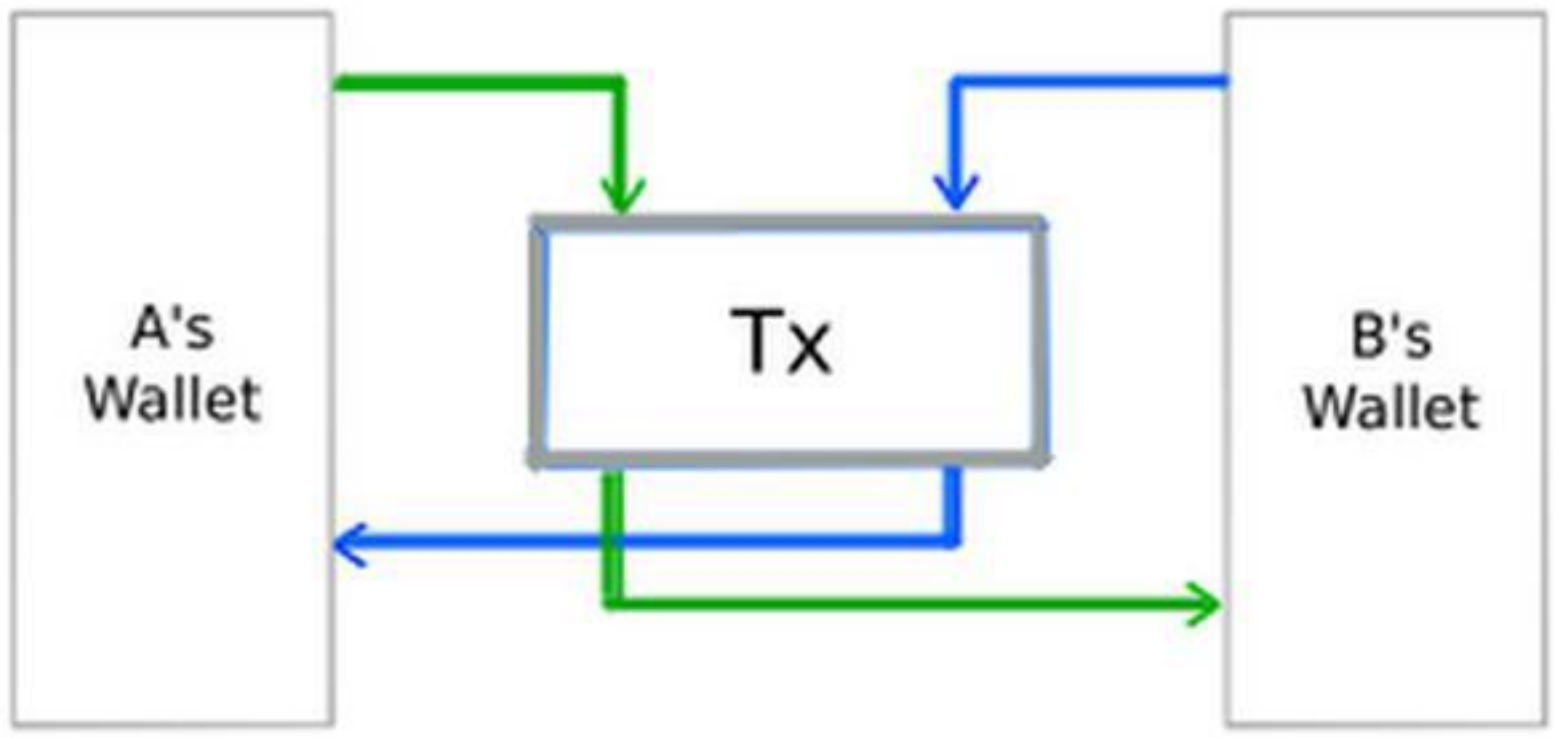
Any type of metadata can be added to a single Satoshi

- Shares
- I_Owe_You
- Gold
- Royalty
- Tickets
- Coupons
- etc.

Gold Coins

$10 000 bill backed by gold

Blockchain Transactions



Decentralized DVP conversion on blockchain

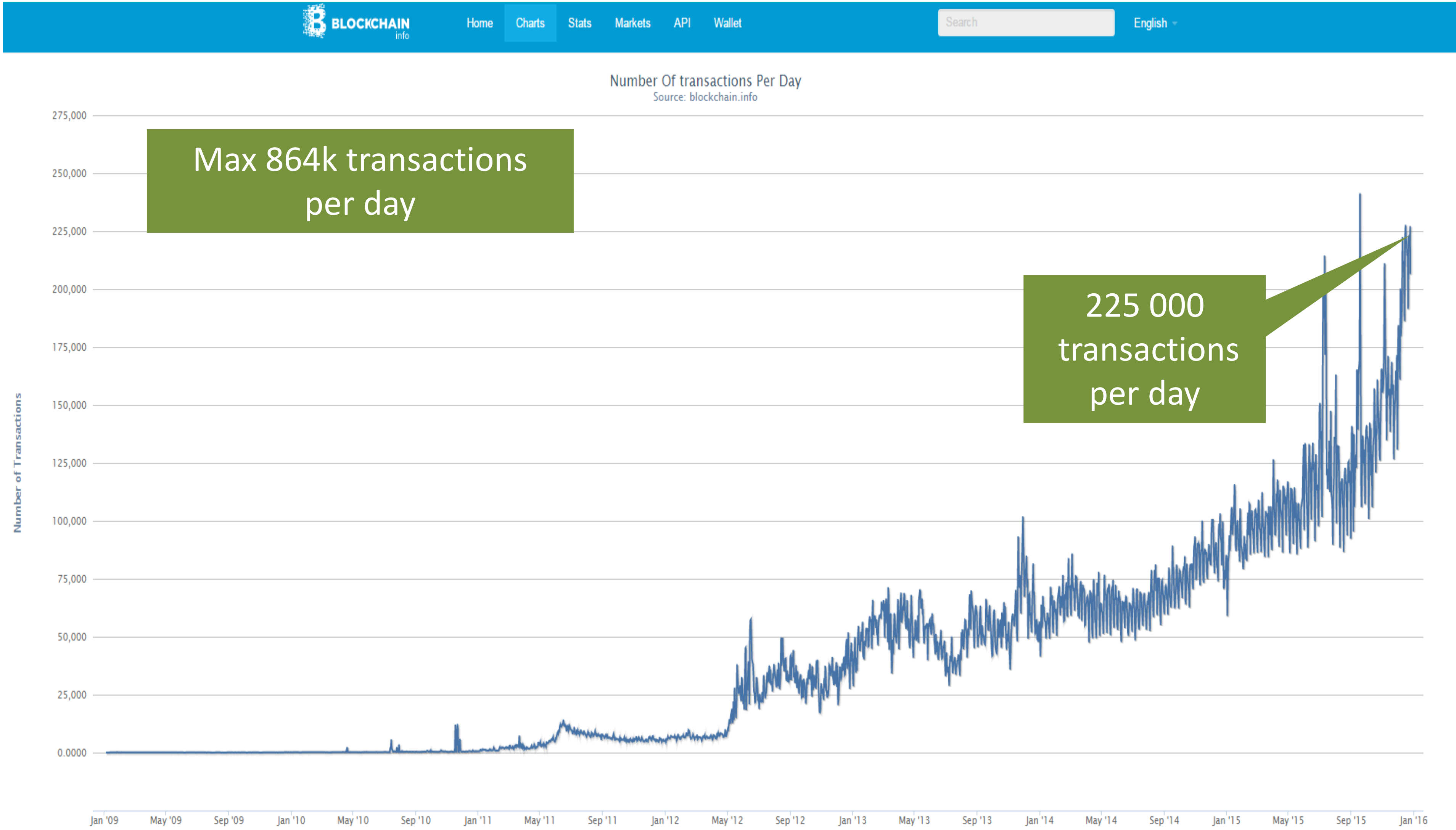
Scalability

Bitcoin Scalability Problems

Problems:

- Transactions aren’t instant
- Micropayments don’t actually work
- “Bitcoin Doesn’t Scale”

Total number of transactions



Number Of transactions Per Day
Source: blockchain.info

Max 864k transactions per day

225 000 transactions per day

PayPal, in contrast, handled around 10 million transactions per day for an average of 115 tps in late 2014

“Bitcoin Doesn’t Scale”

1 Mb blocks:

- 7 transactions per second (250 bytes/transaction)
- 220 mln transaction per year(!)
- Not enough for city, let alone the world

1 Billion transaction per day requires:

- 1.6 GB blocks
- 87 Tb/Year
- Centralization (!)

“Bitcoin Doesn’t Scale”

1 Billion people doing 2 transaction per day:

- 24 GB block
- 3.5 Tb/Day
- 1.27 Pb/Year

Bigger block = Centralization

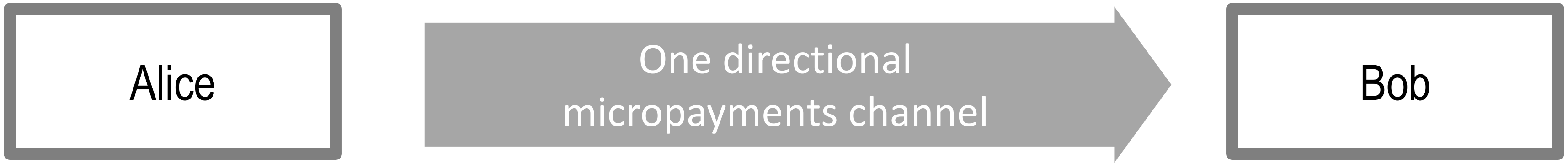
- Very few full nodes
- Very few miners
- De facto inability to validate blockchain

Lykke

Scalability Solutions

1. The SQL database model
   - Very scalable
   - Vulnerable
2. Sidechains
   - Many blockchains with inter-chain transfers
   - Sending funds between chains is two additional transactions
3. Payment channels (Lightning networks)

Offchain Micropayments



Alice

One directional micropayments channel

Bob

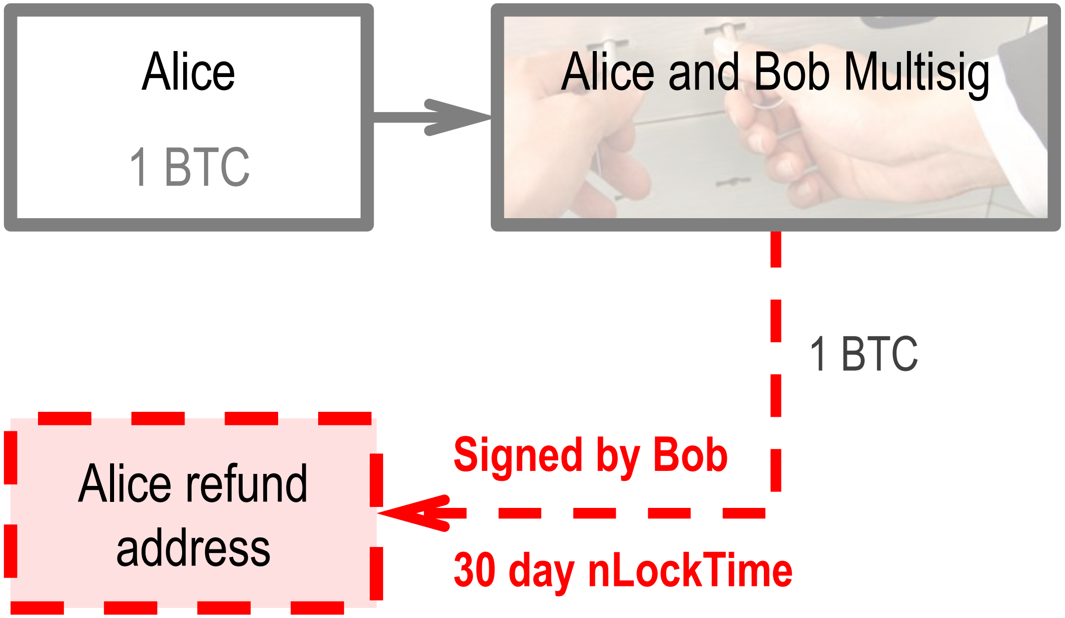
Offchain Micropayments

Alice

Bob

Alice and Bob MultiSig

Offchain Micropayments



Alice

1 BTC

Alice and Bob Multisig

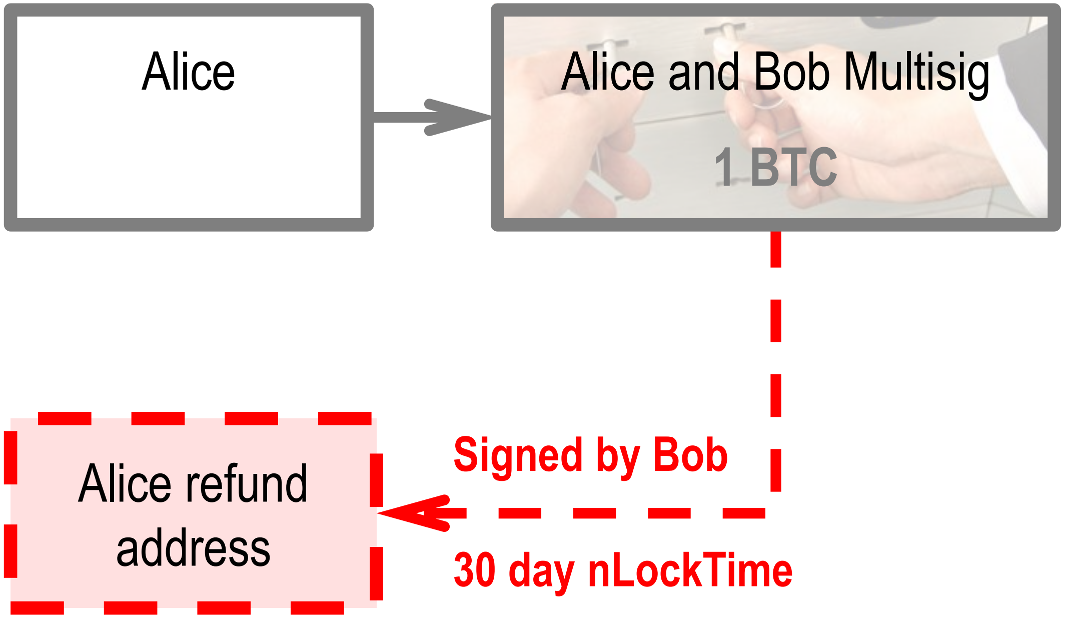
1 BTC

Signed by Bob

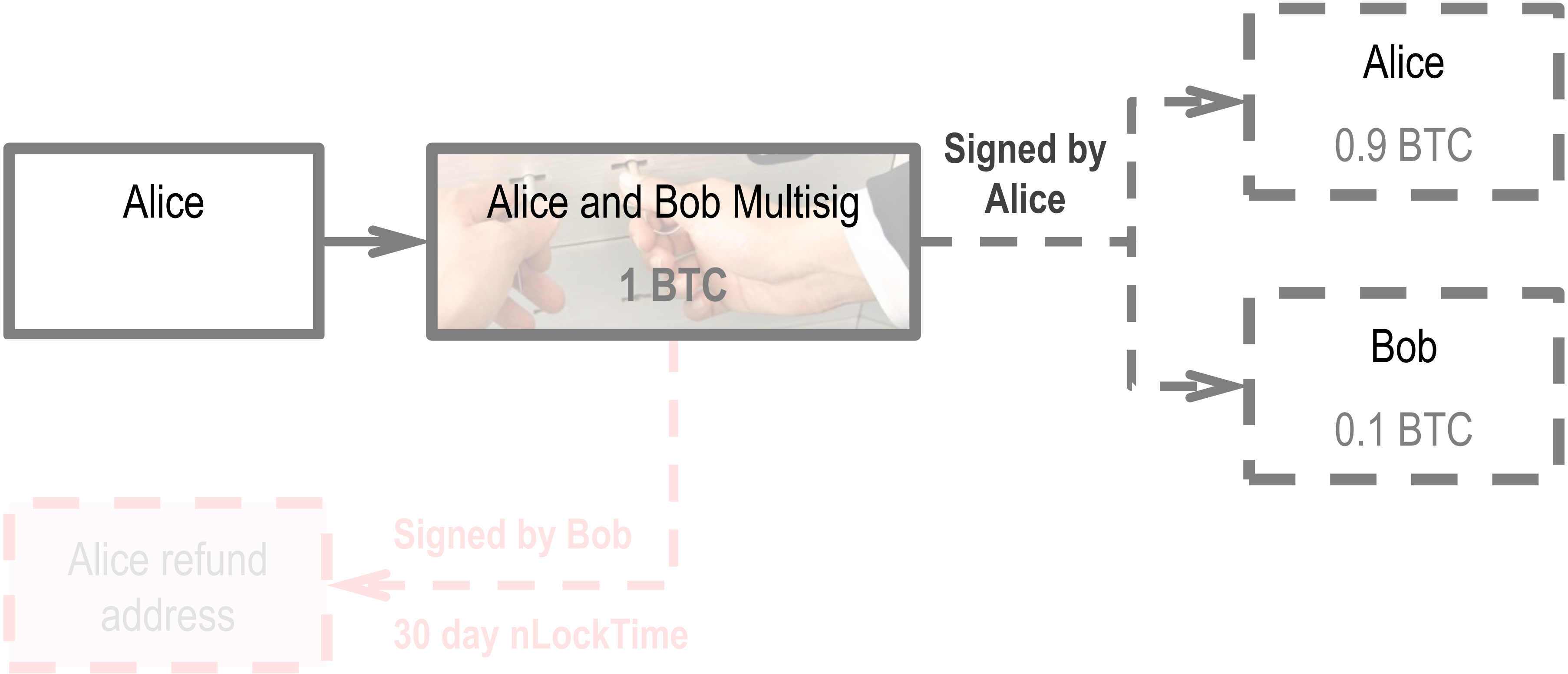
30 day nLockTime

Alice refund address

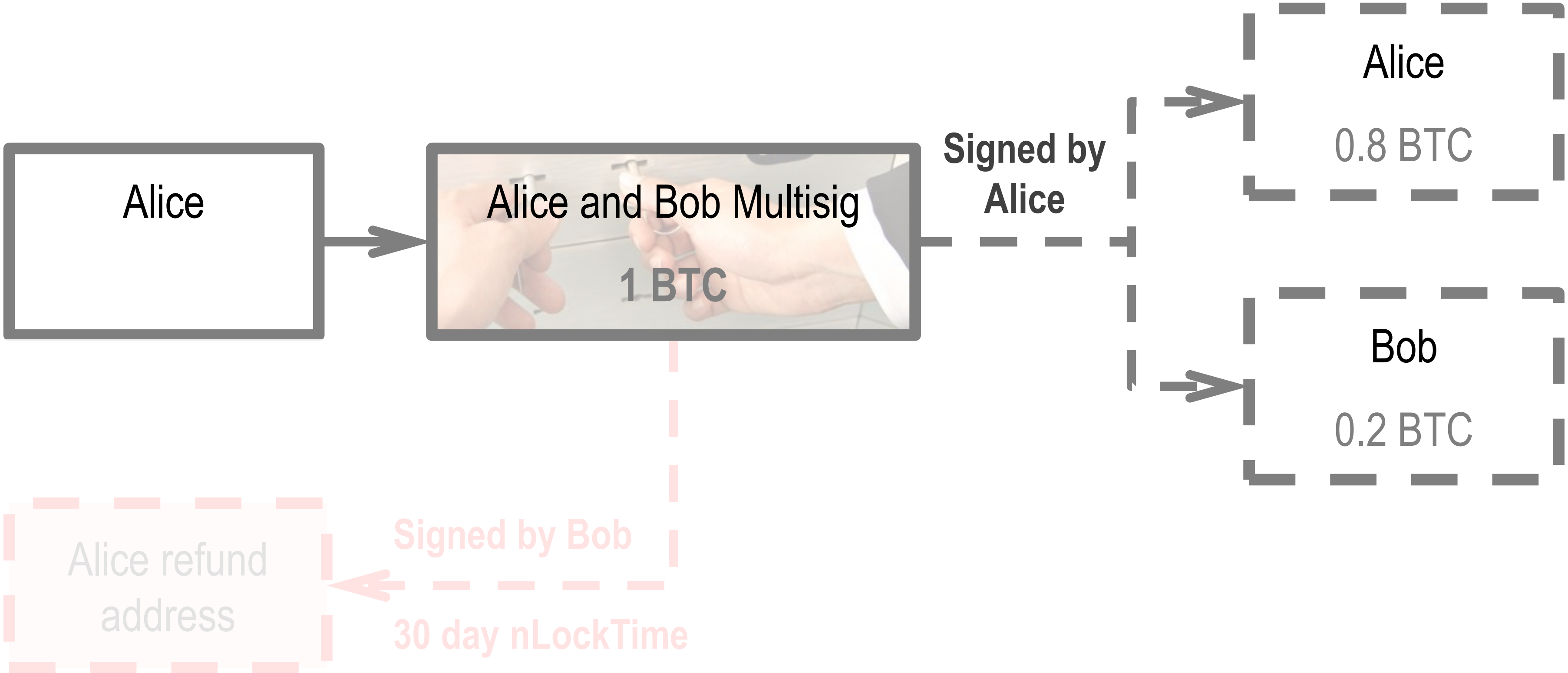
Offchain Micropayments



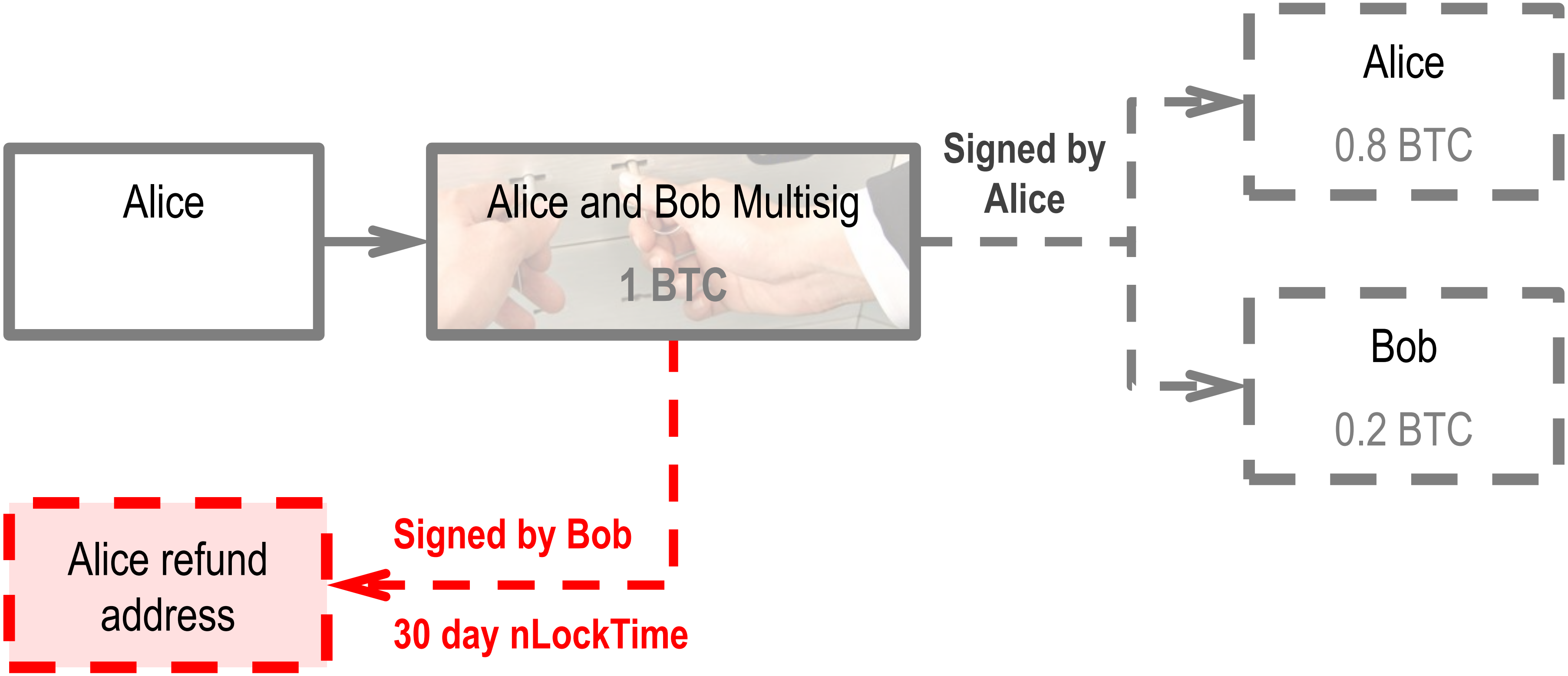
Offchain Micropayments



Offchain Micropayments



Offchain Micropayments



Bitcoin Can Scale

Bitcoin can scale:

- Millions of transactions can be sent offchain instantly and absolutely free
- The latest transaction only should be broadcasted on the blockchain

Blockchain

“The key innovation of digital currencies is the ‘distributed ledger’ which allows a payment system to operate in an entirely decentralised way, without intermediaries such as banks.”

Bank of England – The emergence of digital currencies (2014)

http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf

Blockchain

“The Blockchain Could Disrupt Everything. It has the potential to redefine transactions and the back office of a multitude of different industries. *From banking and payments to notaries to voting systems to vehicle registrations to wire fees to gun checks to academic records to trade settlement to cataloguing ownership of works of art, a distributed shared ledger has the potential to make interactions quicker, less-expensive and safer.”*

Goldman Sachs - Emerging Theme Radar (Dec 2015)

http://www.goldmansachs.com/our-thinking/pages/macroeconomic-insights-folder/what-if-i-told-you/report.pdf

Blockchain

Bitcoin might not change the world, but the blockchain that makes it work, might

Thanks!

Visit Lykke City https://lykkex.com