updated: 24/01 2014

BITCOIN

CRYPTOGRAPHIC TEXTURE

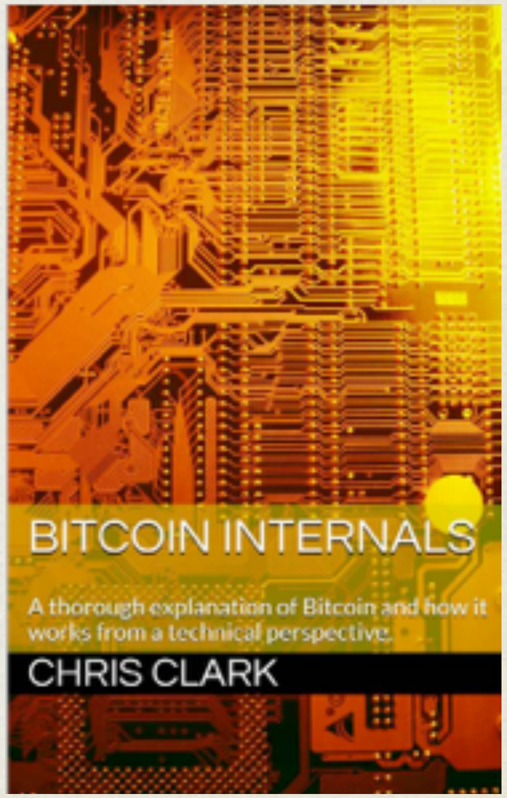
Tomáš Rosa

Raiffeisenbank CZ, December 20th 2013

FAQ

--see also: https://en.bitcoin.it/wiki/FAQ

- **What is a *Bitcoin*?**
  - [B]...a distributed peer-to-peer digital currency system...
  - [b]...a digital record in the public ledger (*BlockChain*) that keeps track of electronic money ownership...
- **Who does operate the *Bitcoin*?**
  - No central company. At least *not **yet***.
  - Spontaneous collaboration of network nodes operated by *miners*. Anybody can join by running an open-source SW.
- **Who has created the *Bitcoin*?**
  - ...NSA, GCHQ, FAPSI, GuoAnBu, Illuminati, ET, The God?
  - All we have is a (perhaps collective) pseudonym *Satoshi Nakamoto*.


BITCOIN INTERNALS
A thorough explanation of Bitcoin and how it works from a technical perspective
CHRIS CLARK

BITCOIN PRIMITIVES

- **The Wallet** - the port of all transactions in BTC and the principal tool to keep them flowing around

- **The BlockChain** - the main, globally replicated ledger and the distributed time-stamping tool to confirm/deny transactions based on a majority voting scheme

- **The Mining** - the force that empowers it all

BTC UNITS

- **standard metric prefixes**
  - 1 BTC … one bitcoin
  - 0,01 BTC … one centibitcoin (cBTC, bitcent)
  - 0,001 BTC … one milibitcoin (mBTC)
  - 0,000 001 BTC … one microbitcoin (μBTC)
- **special unit**
  - 0,000 000 01 BTC … one *satoshi* (the smallest BTC amount)

CONTROLLED SUPPLY

- *“…The reward for solving a block is automatically adjusted so that roughly every four years of operation of the Bitcoin network, half the amount of bitcoins created in the prior 4 years are created…”*

--https://en.bitcoin.it/wiki/FAQ

TOTAL AMOUNT

- Final number of bitcoins issued worldwide is deliberately principally upper-bounded by **21 million BTC**.
  - Expected to closely approach in 2140.
  - In December 2013, after circa 5 years of rapid growth, the total sum was over **12 million BTC**.

--http://blockchain.info/charts/total-bitcoins

MORE PRECISELY

- It is not the number of years what is counted primarily.
- Bitcoin looks for the number of blocks accepted in the BlockChain.
  - The miner’s reward is **halved every 210 000 blocks**.

TOTAL LIMIT REVIEW

- In 2009-2012 (the first 4 years), **10 500 000 BTC** were gained for the first 210 000 blocks.

- Let *k* denote the particular set of **210 000 blocks**.

- Usually, we can see an estimated mapping to years. This assumes the *target adjustment*, so it takes in average **600 seconds** to find a new valid block.

    - *k* = 0 for years **2009 - 2012** (inclusive)

    - *k* = 1 for years **2013 - 2016** (inclusive)

    - *k* = 2 for years **2017 - 2020** (inclusive)

    - ...

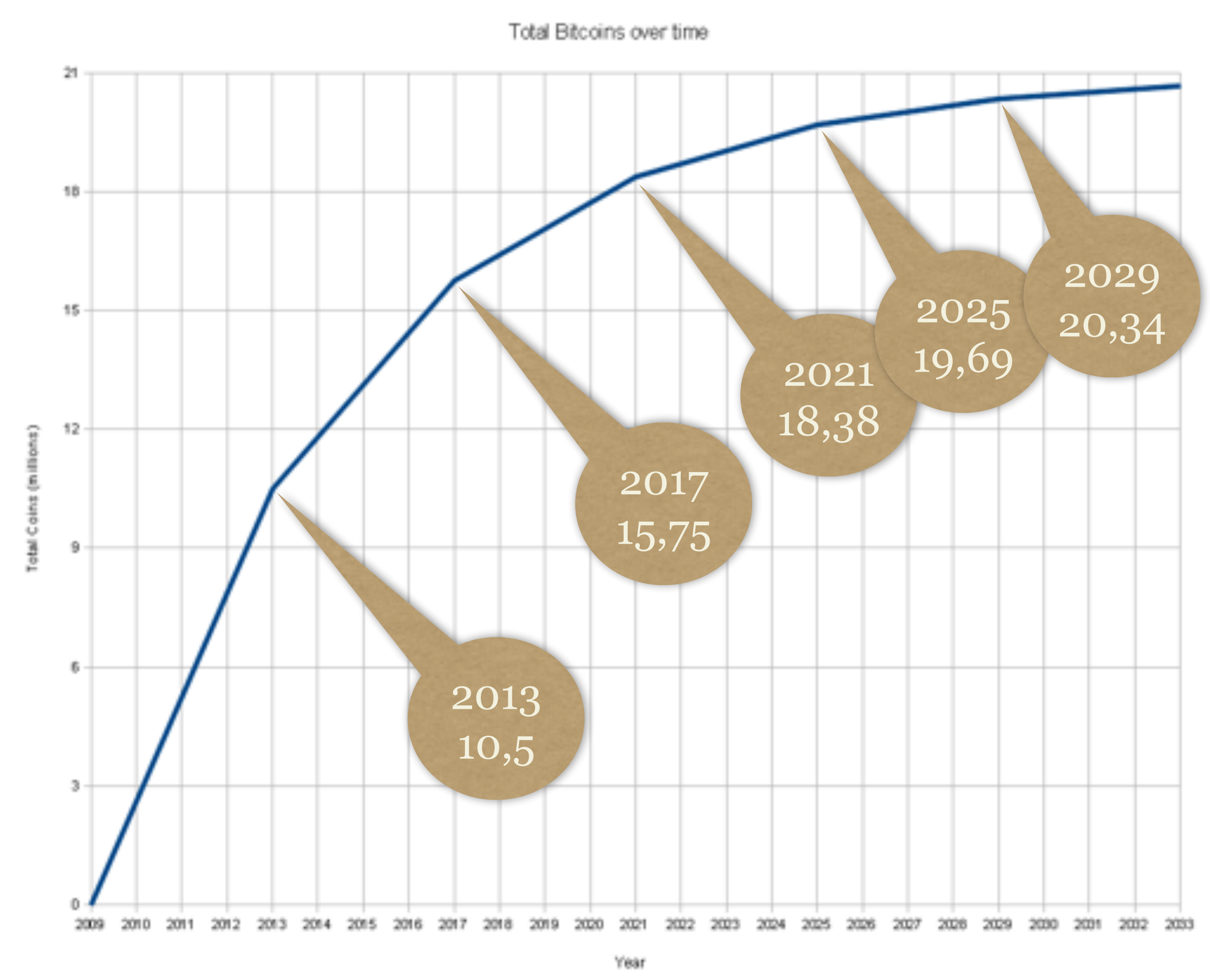
TOTAL LIMIT REVIEW

- The final amount of bitcoins is upper-bounded by the following convergent geometric series

$$10{,}5 \cdot 10^6 \left(1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots\right)$$

$$= \lim_{N \to \infty} \sum_{k=0}^{N} \frac{10{,}5 \cdot 10^6}{2^k}$$

$$= 21\,000\,000$$



2013
10,5

2017
15,75

2021
18,38

2025
19,69

2029
20,34

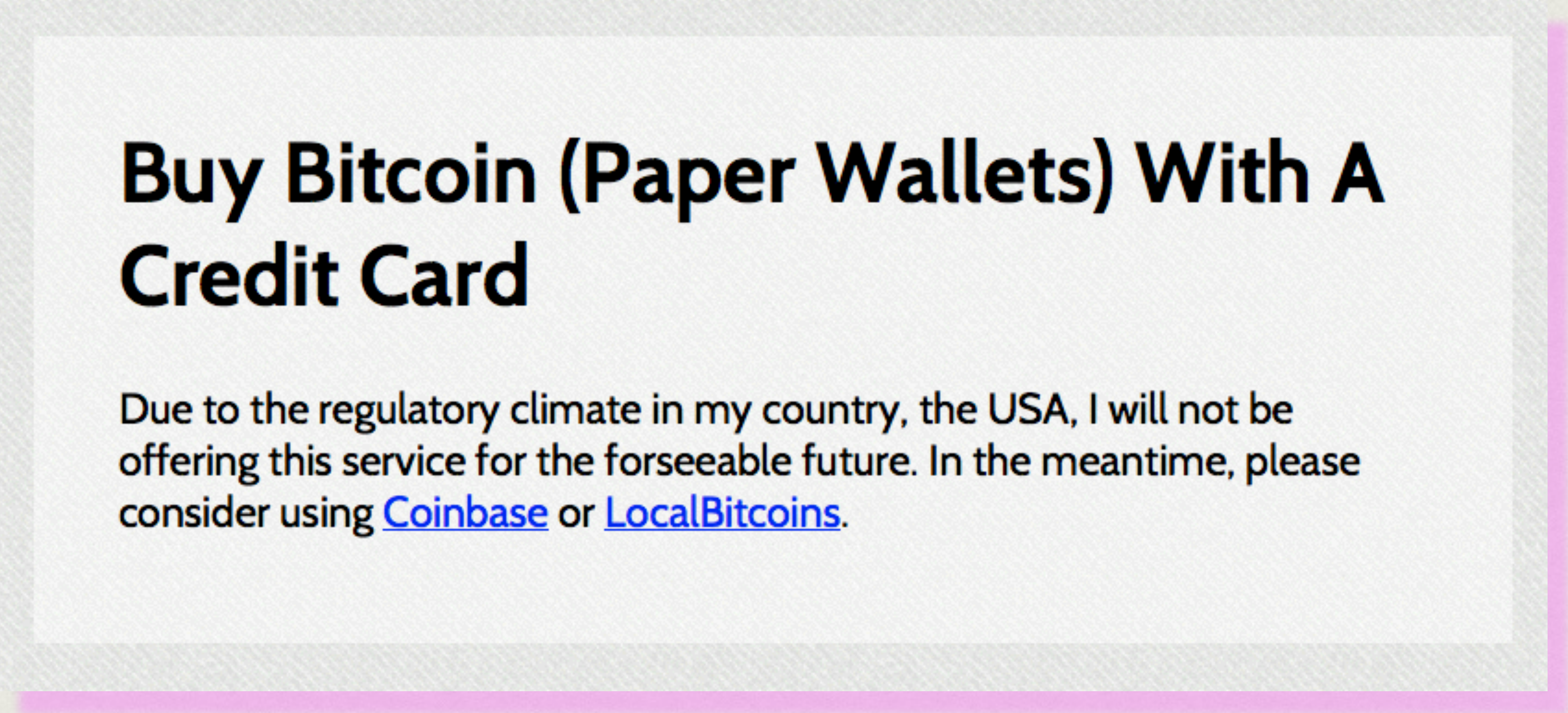
--base graph: https://en.bitcoin.it/wiki/Controlled_Currency_Supply

IN REALITY

- We shall **consider the effect of lost bitcoins**.
    - We will see that a lost private key directly implies lost bitcoins at the particular address.
    - Malware attacks, disasters, somebody passes away without noting their passwords, etc.
- As lower and lower amount of new bitcoins gets produced, the total amount of *disposable* bitcoins can start to decrease.

SHADOW ZONE?

http://buybitcoinwithcreditcard.com/?wiki
November 19th, 2013



Buy Bitcoin (Paper Wallets) With A Credit Card

Due to the regulatory climate in my country, the USA, I will not be offering this service for the forseeable future. In the meantime, please consider using Coinbase or LocalBitcoins.

DISTRIBUTED SYSTEM

- After all, Bitcoin is a kind of distributed system based on strictly symmetric nodes.
    - Because of the symmetry, we can also call it a ***massively replicated system***, since under ideal conditions, all the nodes share the same data and perform nearly identical computations.

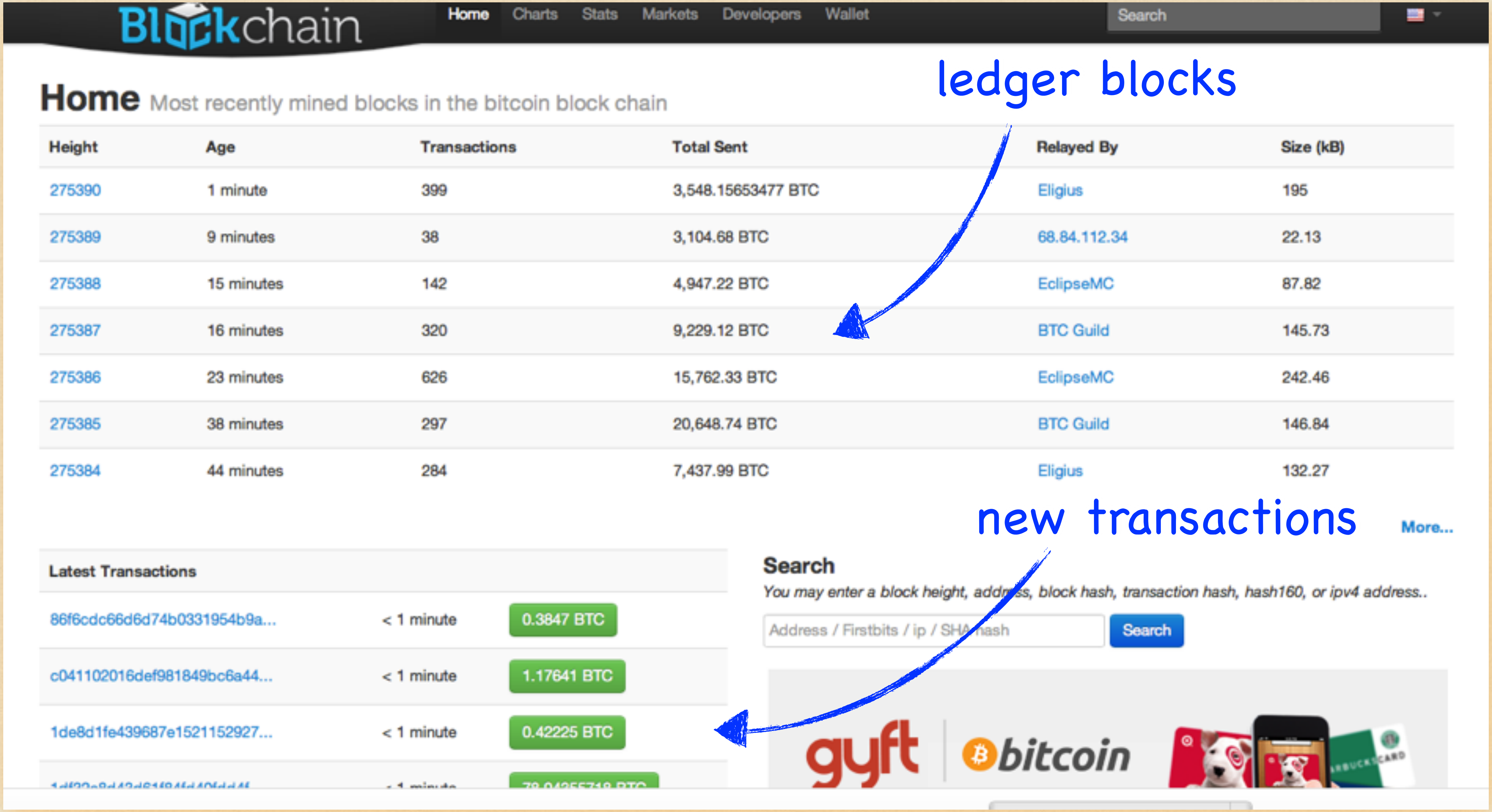
NODES DUTY

- The **voluntary nodes** should be mainly responsible for:
  - spreading the *new transaction broadcast*
  - spreading the *new ledger block broadcast* (BlockChain sync)
  - competing in assembling new ledger blocks, hence creating majority *voting system for txn confirmation* (cf. later on)

HANDS ON

- Certain nodes (*voluntarily* again) provide a user-friendly web view of the Bitcoin distributed system.
    - To name a few: http://blockchain.info, http://blockexplorer.com
    - No to confuse - blockchain.info as a web view versus BlockChain as the shared (massively replicated) Bitcoin ledger.
- You are kindly encouraged to take a tour with these tools...

BLOCKCHAIN.INFO



Home Most recently mined blocks in the bitcoin block chain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
275390	1 minute	399	3,548.15653477 BTC	Eligius	195
275389	9 minutes	38	3,104.68 BTC	68.84.112.34	22.13
275388	15 minutes	142	4,947.22 BTC	EclipseMC	87.82
275387	16 minutes	320	9,229.12 BTC	BTC Guild	145.73
275386	23 minutes	626	15,762.33 BTC	EclipseMC	242.46
275385	38 minutes	297	20,648.74 BTC	BTC Guild	146.84
275384	44 minutes	284	7,437.99 BTC	Eligius	132.27

More...

Latest Transactions		
86f6cdc66d6d74b0331954b9a...	< 1 minute	0.3847 BTC
c041102016def981849bc6a44...	< 1 minute	1.17641 BTC
1de8d1fe439687e1521152927...	< 1 minute	0.42225 BTC
1df32e8d42d61f04fd40fdd4f...	< 1 minute	78.04255718 BTC

Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address..

Address / Firstbits / ip / SHA hash

Search

ledger blocks

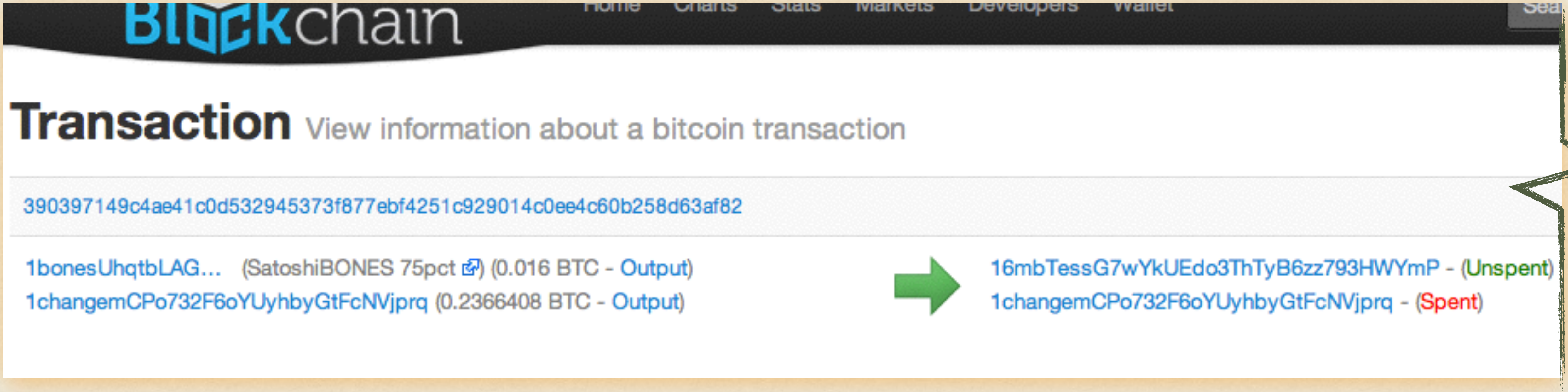
new transactions

SPENDING MY TXN

- We shall understand there is **no single BTC counter** that would say how much money do the client have.
    - Of course, the Wallet application can present the balance. But this is a *derived* value.
- There are just incoming, unspent bitcoin ***transactions outputs*** addressed to the particular Wallet.
    - To spend BTC means to **take some transaction outputs and pass them further** to another Wallet addresses (*M*:*N* relation), possibly returning some money back (i.e. putting ourselves to the recipient list).
    - A *transaction output* is either fully spent or unspent.

A REAL TRANSACTION

- Example transaction joining two former *txns outputs* (received on different Wallet addresses) and passing them to two destinations.
- In fact, certain bitcoins are returned back to "1changem..."
  - Here, we can also see examples of *vanity address* (explained later on).
  - Furthermore, we see inherent privacy issues - the two different addresses were controlled by one subject, weren't they?



Transaction View information about a bitcoin transaction

390397149c4ae41c0d532945373f877ebf4251c929014c0ee4c60b258d63af82

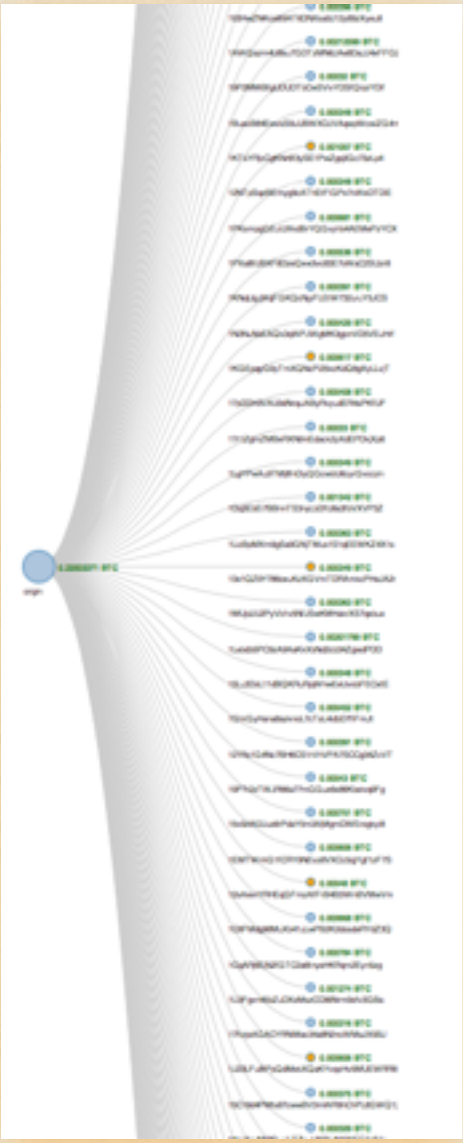
1bonesUhqtbLAG... (SatoshiBONES 75pct) (0.016 BTC - Output)
1changemCPo732F6oYUyhbyGtFcNVjprq (0.2366408 BTC - Output)

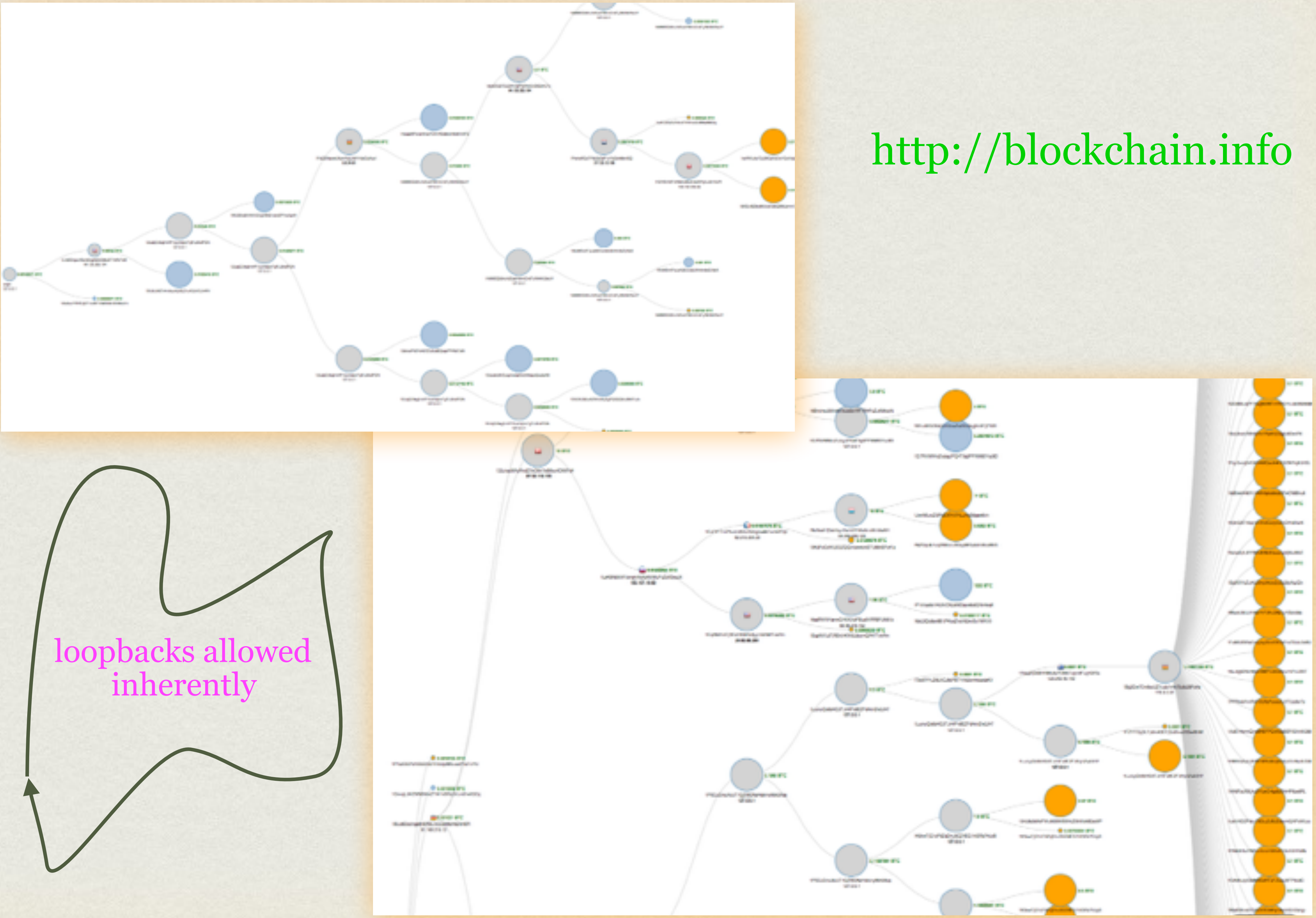
→

16mbTessG7wYkUEdo3ThTyB6zz793HWYmP - (Unspent)
1changemCPo732F6oYUyhbyGtFcNVjprq - (Spent)

--http://blockchain.info

TXN SPOTTING





loopbacks allowed inherently

http://blockchain.info

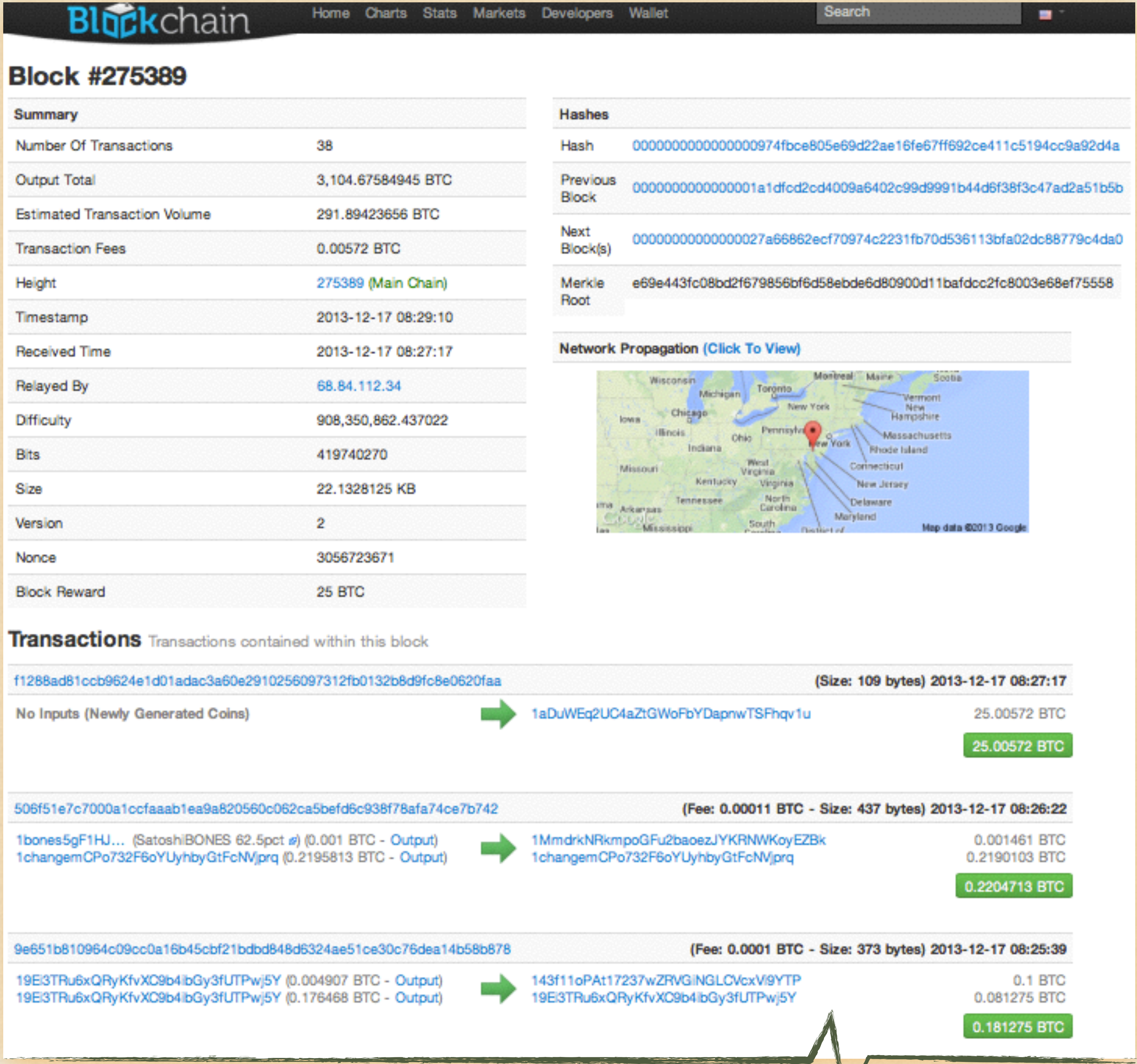
ANONYMITY?

- Whole **transaction list is fully public** (via BlockChain), including sending/receiving addresses, amounts, etc.

- On the other hand, the graph can be highly **obfuscated**, the address is just an ugly hash and one can use many of them, etc.

  - So, it can be practically **annoying enough for AML officers** so to simply let it be and miss something.

  - Theoretically speaking, however, **it is very hard to get any provable privacy** which is bad for almost any company business.



Block #275389

Summary	
Number Of Transactions	38
Output Total	3,104.67584945 BTC
Estimated Transaction Volume	291.89423656 BTC
Transaction Fees	0.00572 BTC
Height	275389 (Main Chain)
Timestamp	2013-12-17 08:29:10
Received Time	2013-12-17 08:27:17
Relayed By	68.84.112.34
Difficulty	908,350,862.437022
Bits	419740270
Size	22.1328125 KB
Version	2
Nonce	3056723671
Block Reward	25 BTC

Hashes	
Hash	0000000000000000974fbce805e69d22ae16fe67ff692ce411c5194cc9a92d4a
Previous Block	000000000000001a1dfcd2cd4009a6402c99d9991b44d6f38f3c47ad2a51b5b
Next Block(s)	0000000000000027a66862ecf70974c2231fb70d536113bfa02dc88779c4da0
Merkle Root	e69e443fc08bd2f679856bf6d58ebde6d80900d11bafdcc2fc8003e68ef75558

Network Propagation (Click To View)

Transactions

Transactions contained within this block

f1288ad81ccb9624e1d01adac3a60e2910256097312fb0132b8d9fc8e0620faa (Size: 109 bytes) 2013-12-17 08:27:17

No Inputs (Newly Generated Coins) → 1aDuWEq2UC4aZtGWoFbYDapnwTSFhqv1u 25.00572 BTC

25.00572 BTC

506f51e7c7000a1ccfaaab1ea9a820560c062ca5befd6c938f78afa74ce7b742 (Fee: 0.00011 BTC - Size: 437 bytes) 2013-12-17 08:26:22

1bones5gF1HJ... (SatoshiBONES 62.5pct) (0.001 BTC - Output)
1changemCPo732F6oYUyhbyGtFcNVjprq (0.2195813 BTC - Output)
→
1MmdrkNRkmpoGFu2baoezJYKRNWKoyEZBk 0.001461 BTC
1changemCPo732F6oYUyhbyGtFcNVjprq 0.2190103 BTC

0.2204713 BTC

9e651b810964c09cc0a16b45cbf21bdbd848d6324ae51ce30c76dea14b58b878 (Fee: 0.0001 BTC - Size: 373 bytes) 2013-12-17 08:25:39

19Ei3TRu6xQRyKfvXC9b4ibGy3fUTPwj5Y (0.004907 BTC - Output)
19Ei3TRu6xQRyKfvXC9b4ibGy3fUTPwj5Y (0.176468 BTC - Output)
→
143f11oPAt17237wZRVGiNGLCVcxVi9YTP 0.1 BTC
19Ei3TRu6xQRyKfvXC9b4ibGy3fUTPwj5Y 0.081275 BTC

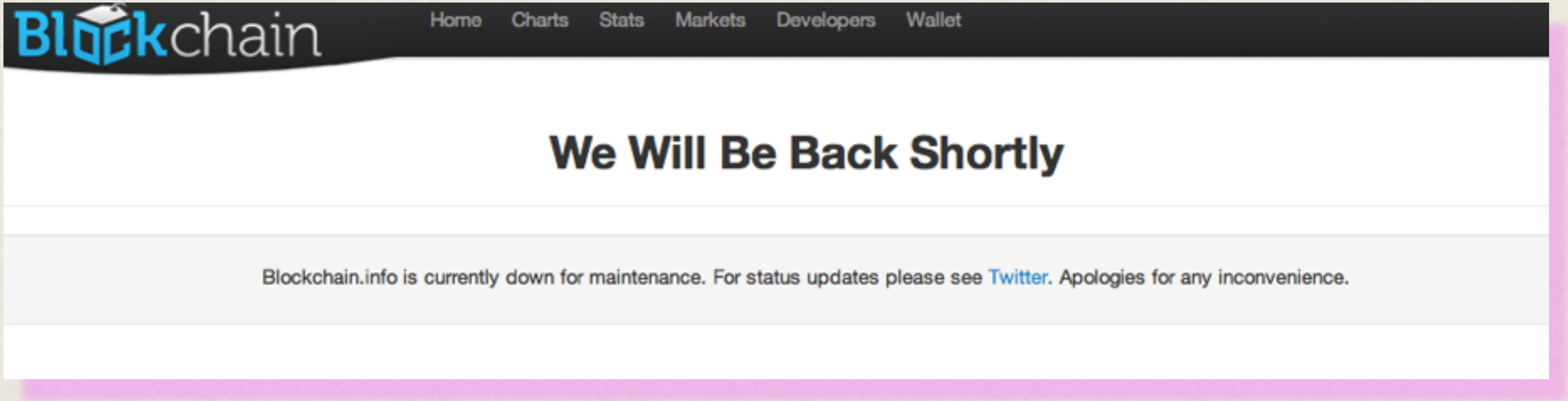
0.181275 BTC

block header

txn list

ALL NICE, BUT...

- We shall understand that almost everything around the Bitcoin is operated in *the best voluntary effort manner*.
  - Corporate IT could bring another level of maturity. But... would it still be that friendly, free, open, nifty Bitcoin? Hardly... Are corporate ITs strong enough to operate the whole Bitcoin when those volunteers give up? How much would it cost and would it be worth it at all? Who will govern the legal part worldwide then? Recall *peer-to-peer* operation is the cornerstone of the majority voting, hence of the whole Bitcoin security (cf. later on).



We Will Be Back Shortly

Blockchain.info is currently down for maintenance. For status updates please see Twitter. Apologies for any inconvenience.

STRIKING MINERS ;-)

—Platinum miners strike in South Africa, JAN 2014

WALLET CRYPTO

- Ensures the *bitcoin transaction output* can be spent by the client with the original recipient's identity only.

- Employs ECDSA over Koblitz elliptic curve “secp256k1”.

--http://www.secg.org/collateral/sec2_final.pdf

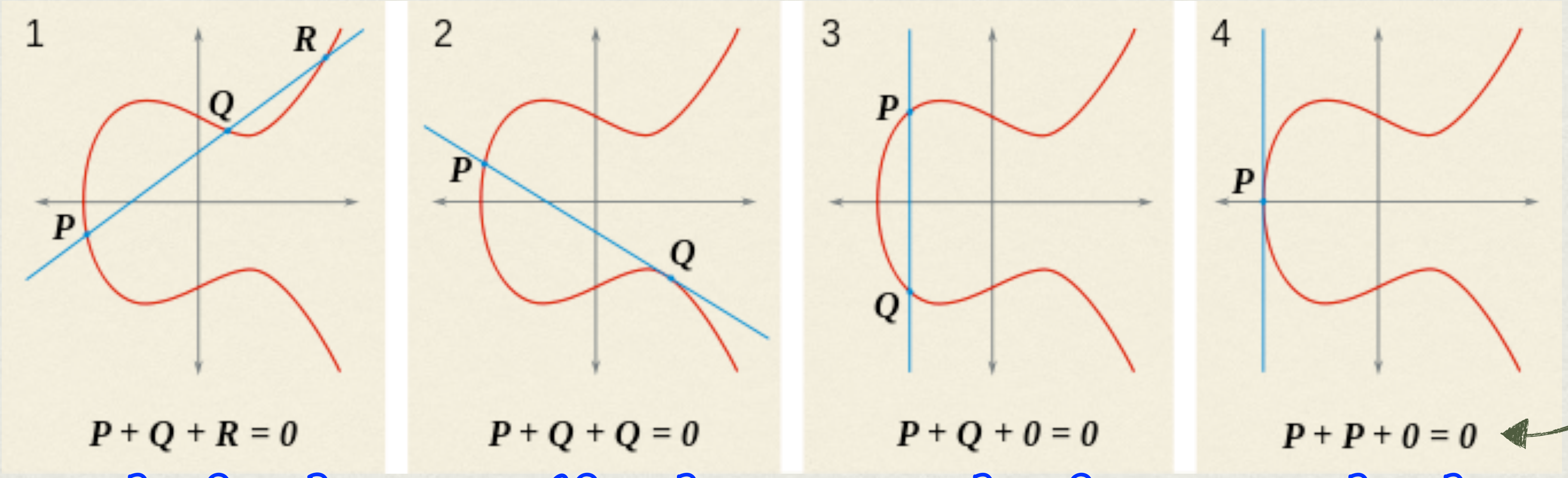
USER IDENTITY

- **Public key**
  - Used to **verify the client identity** with respect to a particular transaction.
  - One-way derivative of this key serves the role of the **client (Wallet) address**.
- **Private key**
  - Used to **prove the client identity** when spending their incoming bitcoin *transaction output*.

ELLIPTIC CURVE

$$E : Y^2 = X^3 + AX + B, \text{ where } 4A^3 + 27B^2 \neq 0$$

group operation



so P + Q = -R

so 2Q = -P

so P = -Q

so P = -P

extra point at infinity O

- In cryptography, we assume *E* over a finite field ***K*** = ***GF***(*p*) or ***K*** = ***GF***(2^m).
- Interestingly, the set of *K*-rational points of *E* together with point ***O*** still form the abelian group.
    - Sometimes, the transition from "classic" crypto is really straightforward. Instead of multiplying integers modulo *p*, we primarily *add* rational points of an elliptic curve. (ECDH, ECDSA)

WHAT ARE THE KEYS ANYWAY?

- **Public key**
  - A particular **point *P* = (*x*, *y*)** on the elliptic curve, where *x* and *y* are elements of the underlying finite field ***K*** - i.e. they are just *two big (~32 B) integers* here.
  - Compressed/uncompressed forms available, since it suffices to **store *x* together with the parity of *y***.
- **Private key**
  - Just another **big integer** (~32 B, from ***Z***) representing the discrete logarithm of the public key ***P***.
    - Or, how many times must be the "reference" point "shuffled" on that curve to get to ***P***.

VANITY ADDRESS

1eskimozYNL62jXa2XSveRyNGst8qr4Bn

- Recall, the client address is a hash of their public key in *Base58Check encoding*.
    - So, it is essentially an ugly-looking random value.
- Anyway, we can keep generating random key pairs until we get **a partly nice address**.
    - We "set" n characters with complexity $O(58^n)$ this way, so it is quite expensive luxury. So the term *vanity address*.
    - **Security risks:**
        - – looking at the vanity part only allows feasible address spoofing!
        - – we shall be careful with services offering generation of vanity key pairs!

KEY EXPLOSION

- To ensure **higher anonymity**, clients tend to generate huge amount of different-looking addresses (i.e. public and private keys).
  - *"...As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner..."*

--Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*

BE AWARE

- There is, however, another principal reason on why to keep generating fresh keys.
- Using a new key pair is **assumed when arguing the resistance** to a double-spending threat (cf. later on).
  - *"...This prevents the sender from preparing a chain of blocks ahead of time..."*

--Satoshi Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*

WALLET SECURITY

- Primarily, it must protect the client private key.
  - If the *key is stolen*, the incoming **bitcoins can be stolen** as well.
  - If the *key is lost*, the incoming **bitcoins are lost**, too.

LOCAL WALLET

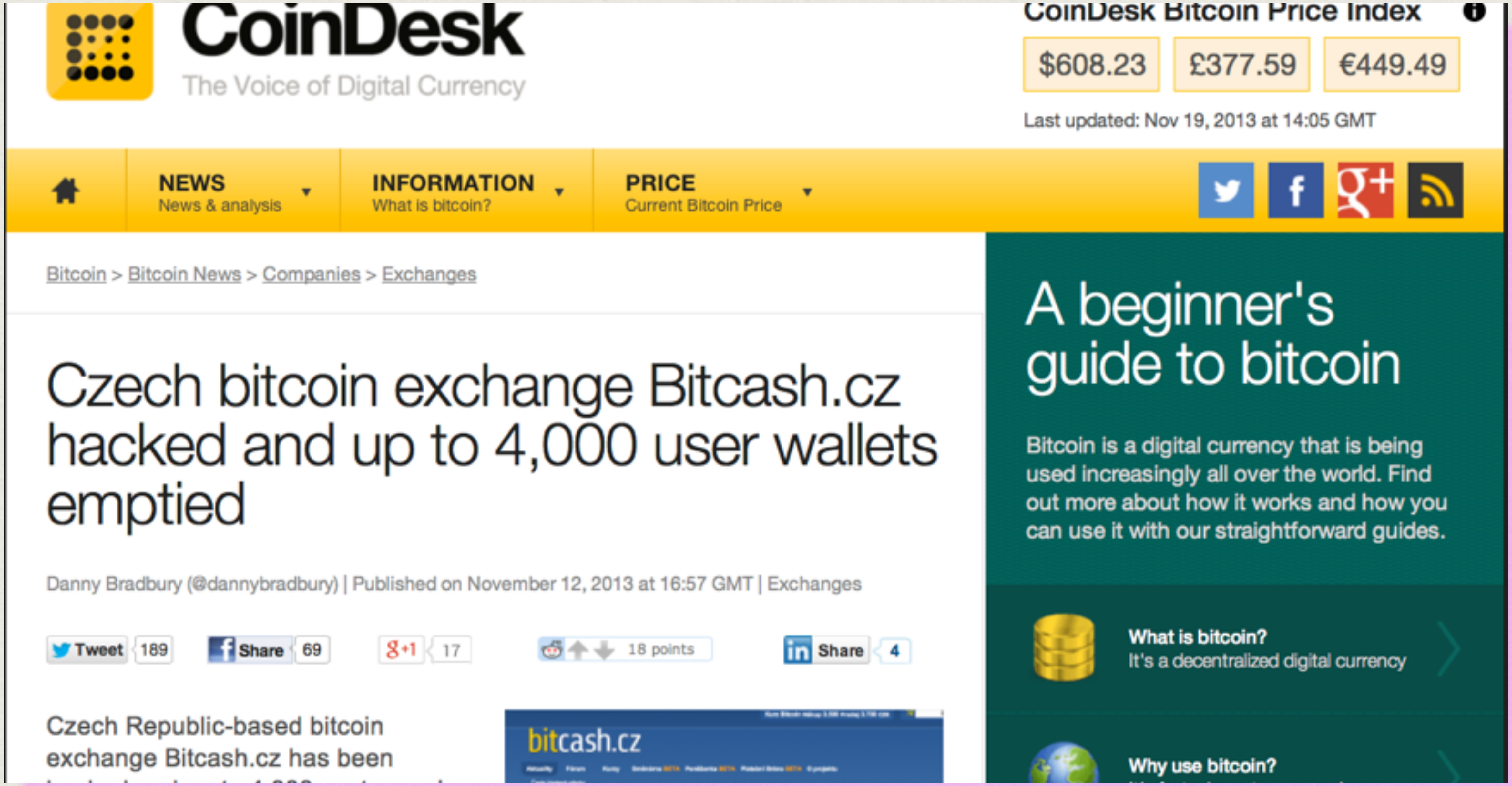
- Application running on a client device with the private key in a password-protected file. Can also work as the *full-fledged node*.
  - Easy target of contemporary **malware**!
  - Furthermore, Android application effectively revealed the private ECDSA keys due to a **weak PRNG**.

    --http://bitcoin.org/en/alert/2013-08-11-android
- Attempts to employ smart cards.
  - This is still vulnerable as long as there is **no trusted display and keypad**.

WALLET AS A SERVICE

- Maintained and encapsulated by a web service **similar to the internet banking**.
  - ***Could be*** a better alternative, provided the web portal uses solid authentication and system security.
  - Unfortunately, this is quite often **not the case**...

QUITE COMMON…



CoinDesk

The Voice of Digital Currency

CoinDesk Bitcoin Price Index

$608.23 £377.59 €449.49

Last updated: Nov 19, 2013 at 14:05 GMT

Bitcoin > Bitcoin News > Companies > Exchanges

Czech bitcoin exchange Bitcash.cz hacked and up to 4,000 user wallets emptied

Danny Bradbury (@dannybradbury) | Published on November 12, 2013 at 16:57 GMT | Exchanges

Czech Republic-based bitcoin exchange Bitcash.cz has been

A beginner's guide to bitcoin

Bitcoin is a digital currency that is being used increasingly all over the world. Find out more about how it works and how you can use it with our straightforward guides.

What is bitcoin?
It's a decentralized digital currency

Why use bitcoin?

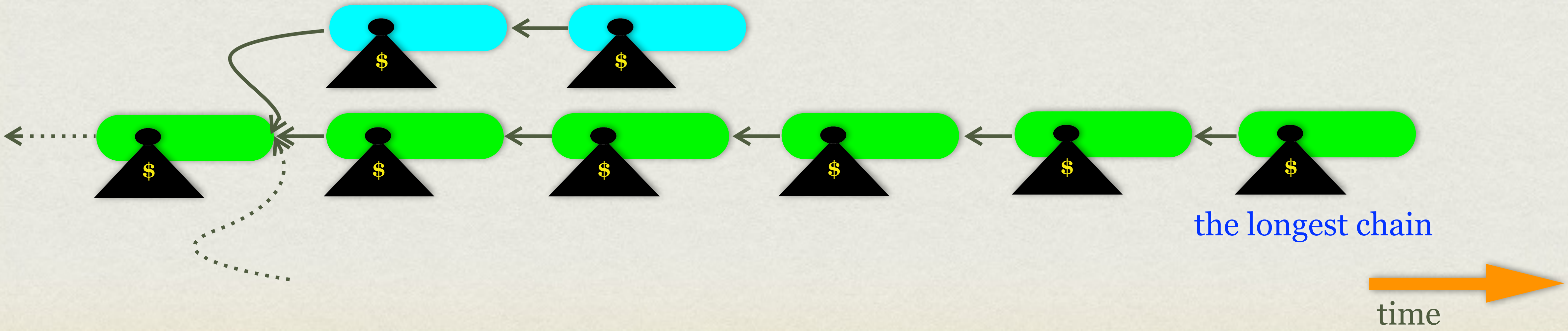
MINING

- *“Mining is the process of adding transaction records to Bitcoin's public ledger* [BlockChain] *of past transactions.”*

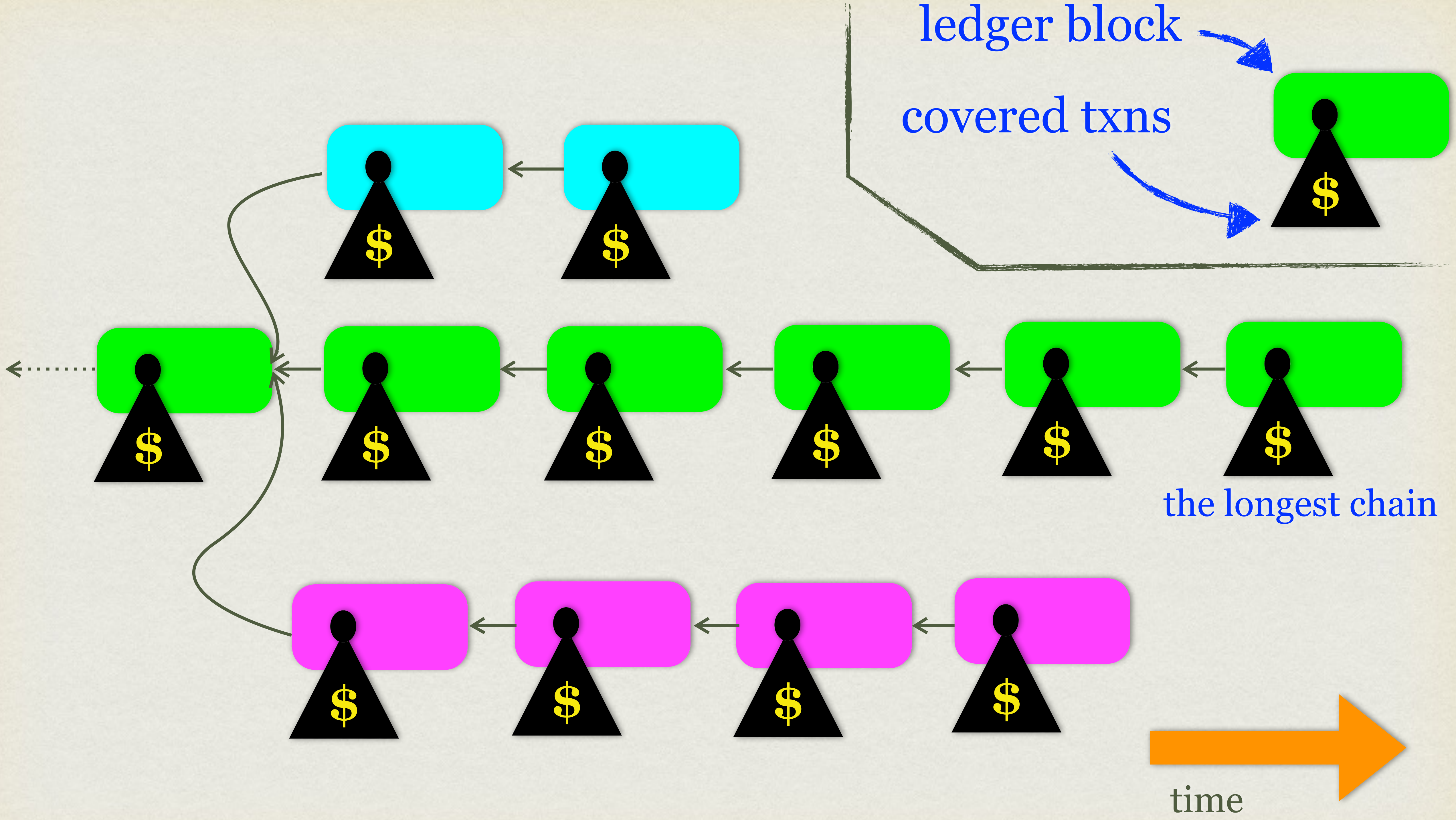
--https://en.bitcoin.it/wiki/Mining

IN OTHER WORDS

- Mining is **using a computing power to vote** for acceptable transactions in the majority voting scheme of the *distributed time-stamp* service called BlockChain.
    - By *trying to make a new block* (in the BlockChain), the mining node votes for the selected transactions to be granted.
    - By *accepting a new block* of a faster competitor, the nodes votes for this block (incl. the transactions covered there) is correct (i.e. they agree with it).
        - To accept the block means to start searching for a new block following this one instead of the former last block.

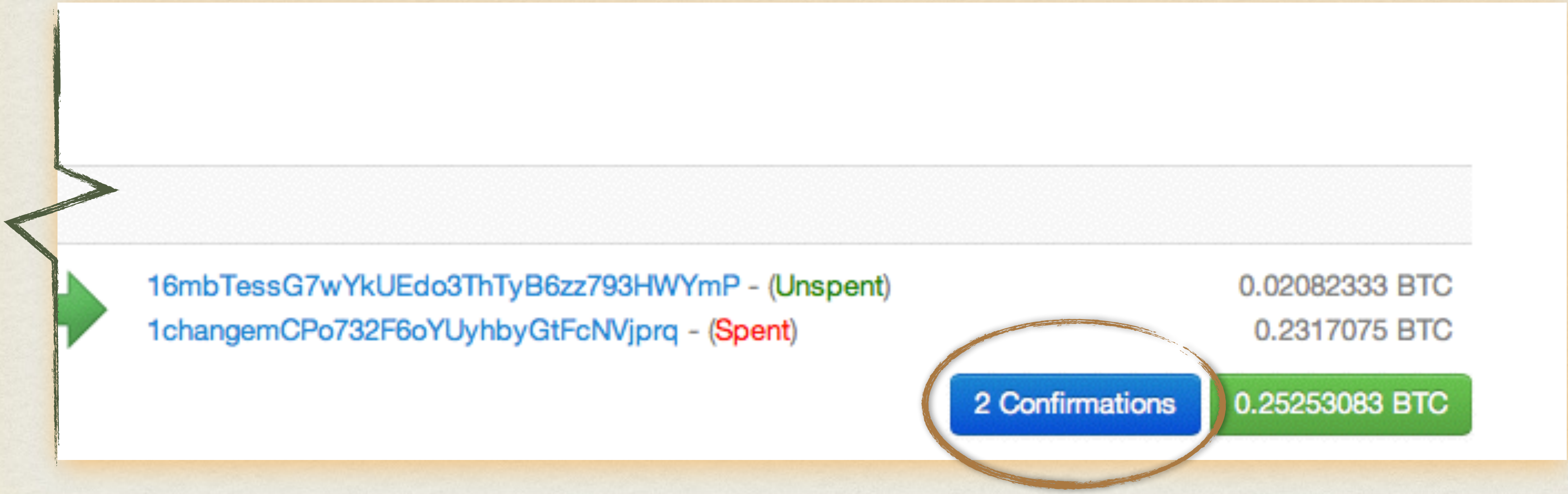


DISTRIBUTED TIME-STAMPING



IN PRACTICE

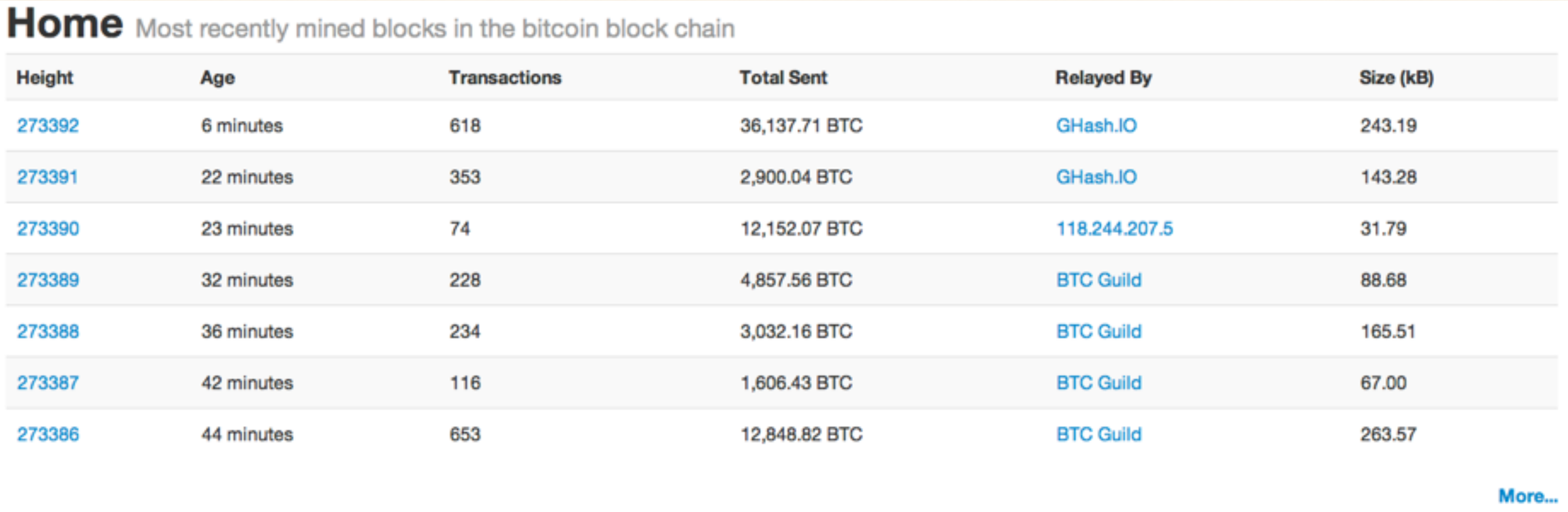
- This is actually a second part of the sample transaction view presented a few slides above.
  - This transaction was apparently confirmed by two blocks - one primary and another one following it.



16mbTessG7wYkUEdo3ThTyB6zz793HWYmP - (Unspent) 0.02082333 BTC

1changemCPo732F6oYUyhbyGtFcNVjprq - (Spent) 0.2317075 BTC

BLOCKCHAIN GROW



Home Most recently mined blocks in the bitcoin block chain

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
273392	6 minutes	618	36,137.71 BTC	GHash.IO	243.19
273391	22 minutes	353	2,900.04 BTC	GHash.IO	143.28
273390	23 minutes	74	12,152.07 BTC	118.244.207.5	31.79
273389	32 minutes	228	4,857.56 BTC	BTC Guild	88.68
273388	36 minutes	234	3,032.16 BTC	BTC Guild	165.51
273387	42 minutes	116	1,606.43 BTC	BTC Guild	67.00
273386	44 minutes	653	12,848.82 BTC	BTC Guild	263.57

More...

CORE EVENTS

- We define the following events and corresponding probabilities:
  - ***H*, Pr[*H*]** is the *core event* the honest nodes (collectively) find a new block in an observable *time instant*
  - ***A*, Pr[*A*]** is the *core event* attackers (collectively) find a new block in a *time instant*

PROOF-OF-WORK (POW)

- Connects the particular vote with certain amount of computing power that had to be spent.

- **To vote means to compete in producing a new block**.

  - For voting, it is not so important who in particular has produced the block.

  - It is the competition under common rules that shall form the unit force of the honest nodes (against the dishonest ones).

  - It *collectively* grounds the $\Pr[H]$ and $\Pr[A]$ defined above.

FURTHERMORE

- Proof-of-Work hash is actually an **easy-to-verify mark** the voting model based on Pr[H] and Pr[A] really applies for the particular BlockChain subgraph.
    - By checking the hash code mark (cf. later) and assuming SHA-256 is not broken, we are ensured the particular *block emission indeed follows our model probabilities*.

POW CRYPTO PUZZLE

- To enforce Pr[H] and Pr[A] distributions, a kind of *cryptographic puzzle* must be solved for the new block to get accepted (i.e. for others to start producing new blocks behind it).
  - In particular, SHA-256(SHA-256(*block_header*)) < *target*, where *target* is a variable boundary.
  - Furthermore, we define: $difficulty = 65535 * 2^{208} / target$.
  - The *target* is adjusted collectively after 2016 blocks in such way that it takes approximately 600 seconds to find a new block (*collectively*, under a Poisson process variant).

CURRENT TARGET

DEC 6th 2013

- Current target: http://blockexplorer.com/q/hextarget
  - 00 00 00 00 00 00 00 0**6 12 42** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (HEX)
- Current difficulty: http://blockexplorer.com/q/getdifficulty
  - 707 408 283.0515
- Current chance per one try: http://blockexplorer.com/q/probability
  - $\textit{target}*2^{-256} \cong 0.000\ 000\ 000\ 000\ 000\ 000\ 3291268939287241815545848044877175198 < 10^{-18}$

CURRENT TARGET

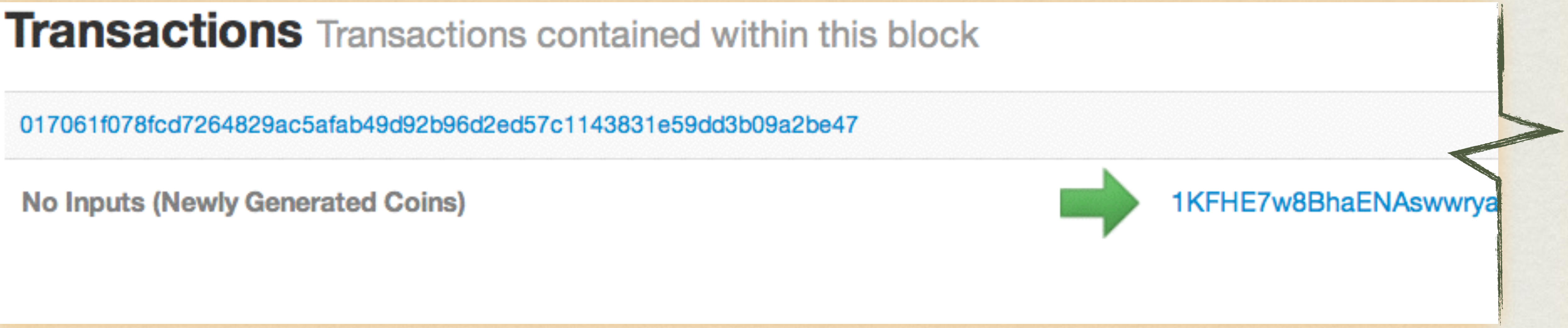
JAN 24th 2014

- Current target: http://blockexplorer.com/q/hextarget
  - 00 00 00 00 00 00 00 **02 66 66** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 (HEX)
- Current difficulty: http://blockexplorer.com/q/getdifficulty
  - 1 789 546 951.0532
- Current chance per one try: http://blockexplorer.com/q/probability
  - *target**$2^{-256} \cong$ 0.000 000 000 000 000 000 1301039298260155108698243875409161773 $< 10^{-18}$

MINER’S REWARD

- The creator of each new block in the BlockChain has the right to insert a special *coinbase transaction* addressed to their wallet.
    - The amount is fixed for a time period. It was BTC 25 in December 2013.
    - This is the only way **new bitcoins** are born.
    - For safety, **100 confirmations** is required to grant the *coinbase transaction.*
- Furthermore, the creator also takes (yet-optional) **transaction fees**.
    - The positive difference in between the sum of input and output transactions.
    - This ranges in mBTC, so several orders of magnitude bellow the new bitcoins reward.
    - Later on, however, it may become dominant source of income.

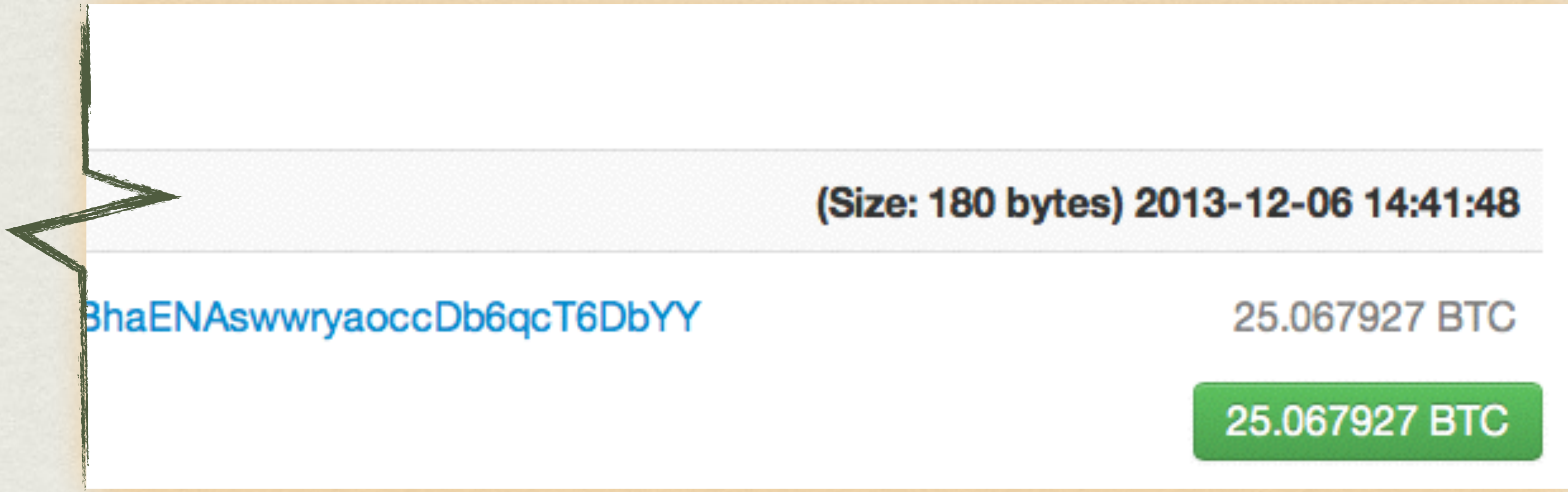
COINBASE TXN



Transactions Transactions contained within this block

017061f078fcd7264829ac5afab49d92b96d2ed57c1143831e59dd3b09a2be47

No Inputs (Newly Generated Coins) → 1KFHE7w8BhaENAswwrya



(Size: 180 bytes) 2013-12-06 14:41:48

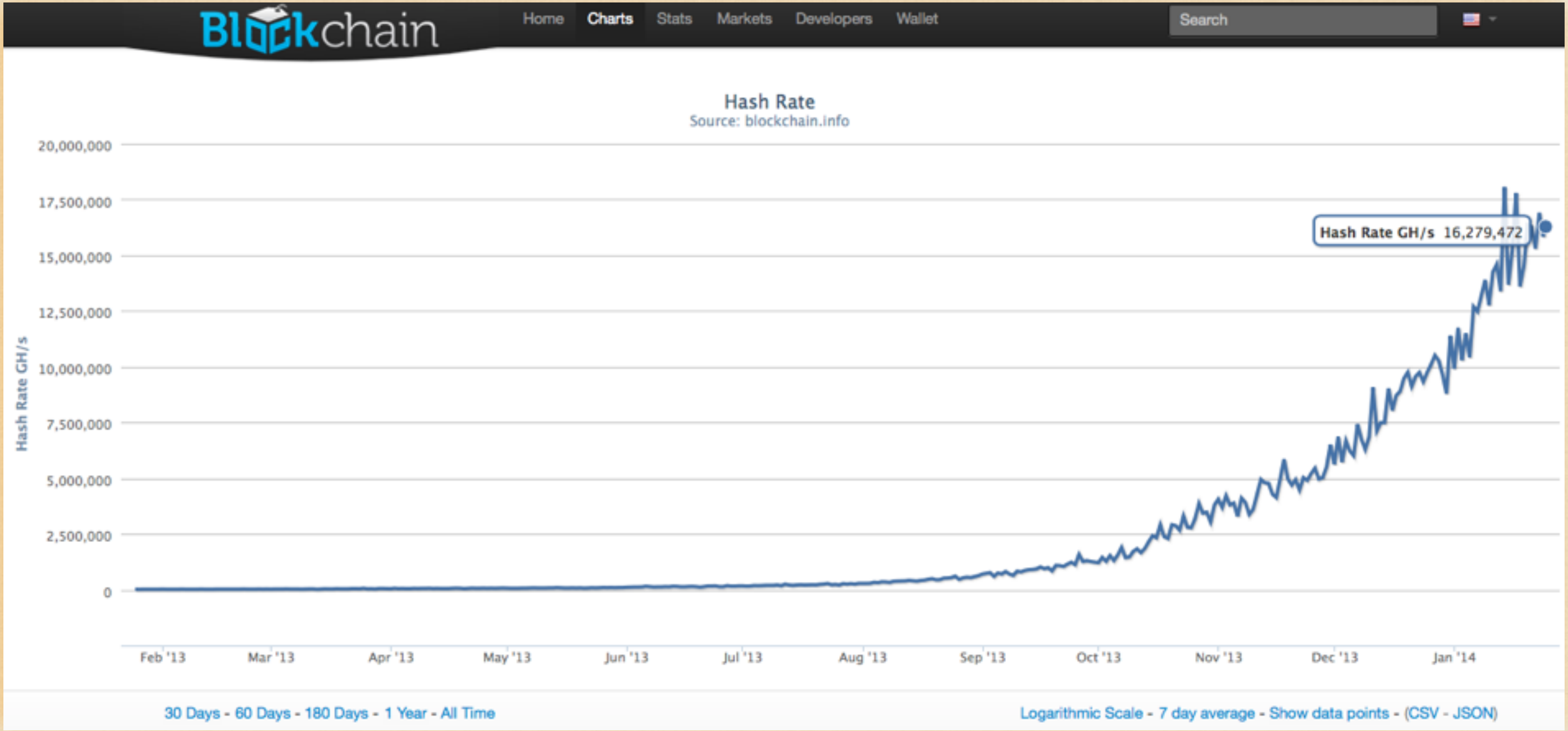
BhaENAswwryaoccDb6qcT6DbYY 25.067927 BTC

25.067927 BTC

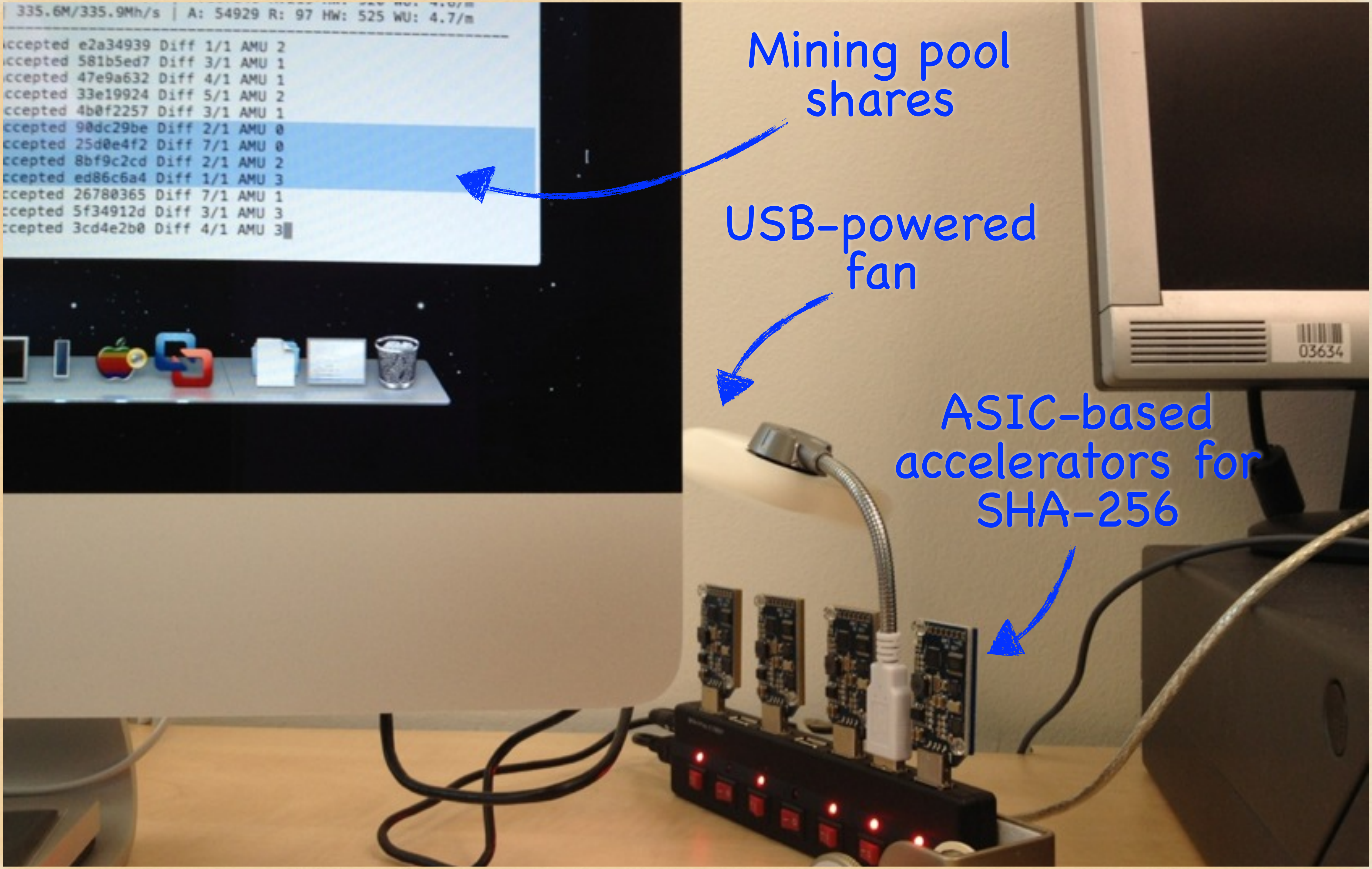
MINING POOLS

- From the Bitcoin viewpoint, joining even as a single miner makes sense, since the majority voting is all about *collective power*.
- On the other hand, single miner can hardly expect to get any reward soon (it is just a big, big lottery game).
  - So, miners usually join indirectly via *mining pools*.
  - The reward is then divided in according to the *power share* ratio.
  - Much smaller than the block reward, but it is a kind of stable income.
- From the voting viewpoint, however, such **concentration is dangerous**.
  - Who controls those **mining pools with such a strong vote**?

HASH RUSH


Blockchain
Home
Charts
Stats
Markets
Developers
Wallet
Search
Hash Rate
Source: blockchain.info
Hash Rate GH/s
20,000,000
17,500,000
15,000,000
12,500,000
10,000,000
7,500,000
5,000,000
2,500,000
0
Hash Rate GH/s 16,279,472
Feb '13
Mar '13
Apr '13
May '13
Jun '13
Jul '13
Aug '13
Sep '13
Oct '13
Nov '13
Dec '13
Jan '14
30 Days - 60 Days - 180 Days - 1 Year - All Time
Logarithmic Scale - 7 day average - Show data points - (CSV - JSON)

EVERYTHING COUNTS



```
335.6M/335.9Mh/s | A: 54929 R: 97 HW: 525 WU: 4.7/m
----------------------------------------------------------
ccepted e2a34939 Diff 1/1 AMU 2
ccepted 581b5ed7 Diff 3/1 AMU 1
ccepted 47e9a632 Diff 4/1 AMU 1
ccepted 33e19924 Diff 5/1 AMU 2
ccepted 4b0f2257 Diff 3/1 AMU 1
ccepted 90dc29be Diff 2/1 AMU 0
ccepted 25d0e4f2 Diff 7/1 AMU 0
ccepted 8bf9c2cd Diff 2/1 AMU 2
ccepted ed86c6a4 Diff 1/1 AMU 3
ccepted 26780365 Diff 7/1 AMU 1
ccepted 5f34912d Diff 3/1 AMU 3
ccepted 3cd4e2b0 Diff 4/1 AMU 3
```

Mining pool shares

USB-powered fan

ASIC-based accelerators for SHA-256

SOMEBODY…

- …who likes conspiracy theories can even argue the new block competition together with the particular proof-of-work scheme closely resembles **massively parallel cryptanalysis** based on *distinguished points*.
    - Of course, *this was the intent* as the PoW is nothing but a cryptanalytic problem that we believe there is no better way to solve it than using a brute force.
    - There is no clear evidence this whole effort should have any other significance.
    - It is even unclear of what should be the target. Random collision of SHA-256, or something hidden behind its design?
    - Well, it is **nothing but a fun idea**…

ANYWAY

- We shall take a lesson of what can be done by carefully motivating people on the internet to perform a distributed computation.
  - Evidently, the "Bitcoin rush" outperforms any other distributed cryptanalytic experiment we have done so far.
  - The whole Bitcoin mining power is **over 2^{53} *double* SHA-256 per second** and still increasing!
    - Imagine such power applied for password cracking...
    - ...or SHA-1 collision searching...

MAJORITY VOTING

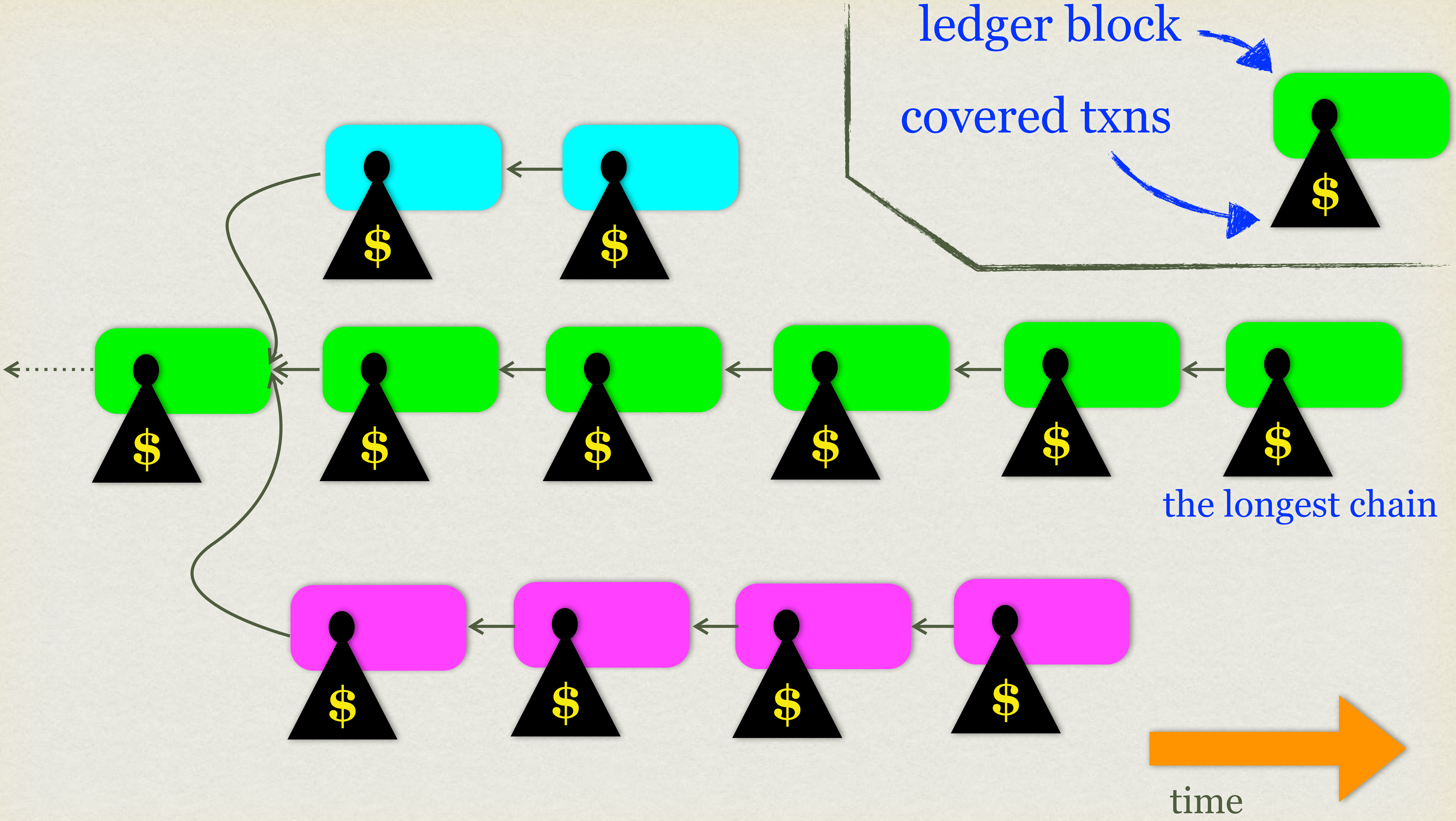
- Let us assume a client who is awaiting a bitcoin transaction.
- Such a client shall **accept the transaction only if**:

  i) it is covered by a ledger block that belongs to the *longest path* in the BlockChain,

  ii) the covering block is then *followed by several other* blocks in the longest BlockChain path.

- This all is to prevent the transaction gets denied later on.

RECALL



DOUBLE SPENDING

- An attacker sends a bitcoin transaction to the victim.
  - In parallel, the attacker (*group of attackers*) keeps generating blocks sequence that covers **spending the same *transaction output* again** (now, in a different way).
- Meanwhile, the victim gets ensured by the majority vote the former transaction is valid and delivers their promise.
  - After a while, the attacker pushes the **alternate blocks sequence as the longest tail** in the BlockChain.
  - Suddenly, the former transaction is invalid.

THE RACE IS ON!

- Let us assume the client accepts the majority vote **after having seen *z* blocks** in the BlockChain covering the transaction.
  - The first block covers it directly, the following blocks confirm recurrently all the previous blocks.
- So the attacking group has to present **the parallel chain that eventually outperforms the honest chain** which is already *z* blocks long in that time.
  - Of course, the attackers keep working on their chain heavily, despite delaying its release.

CHANCE TO WIN

- Let us denote ***Q*(*p*, *q*, *z*)** the probability that **the attacking group will eventually win the race**, where
  - *p*, *q* is the probability the last block observed was made by honest nodes or attackers, respectively (cf. the channel model later on)
  - *z* is the number of blocks the client waits for before accepting the Bitcoin network majority vote

$$Q(p,q,z) \leq \sum_{k=0}^{\infty} e^{-\lambda} \frac{\lambda^k}{k!} \cdot \begin{cases} \left(\frac{q}{p}\right)^{z-k} & \text{if } z>k \\ 1 \text{ otherwise} \end{cases}$$

$$\lambda = z\frac{q}{p}$$

DISSECTING Q

we
deal with necessary
conditions

$$Q(p,q,z) \leq \sum_{k=0}^{\infty} e^{-\lambda} \frac{\lambda^{k}}{k!} \cdot \begin{cases} \left(\frac{q}{p}\right)^{z-k} & \text{if } z>k \\ 1 \text{ otherwise} & \end{cases}$$

$$\lambda = z\frac{q}{p}$$

mean #blocks
found when the
honests got *z* blocks

attackers have
already prepared *k*
blocks

catch up for the
remaining
max {*z*-*k*, 0} blocks

EVENTS REVISITED

- We define the following events and corresponding probabilities:

  – ***H*, Pr[*H*]** is the *core event* the honest nodes (collectively) find a new block in an observable *time instant*

  – ***A*, Pr[*A*]** is the *core event* attackers (collectively) find a new block in a *time instant*

  – ***N*, Pr[*N*]** is the *observable event* a new block (from either side) is reported in Bitcoin net (in a *time instant*)

  – ***C*, Pr[*C*]** is the *observable event* of a clear state, i.e. there is no new block announced (in a *time instant*)

PROBABILISTIC POWER

- We are **not** counting *double SHA-256* computations directly.
  - To get the honest/attacking mean values to the same ground, we count ***time instants*** (Δt) instead.
- The honest and attacking nodes total power is represented by their ***computing mass coefficient*** γ and α, respectively.
  - These coefficients describe the ratio of #double-SHA-256 finished in Δt. So, for a current Bitcoin *target*, we have

$$\Pr[H] = 1 - (1 - \frac{target}{2^{256}})^{\gamma}$$

$$\Pr[A] = 1 - (1 - \frac{target}{2^{256}})^{\alpha}$$

SOUNDNESS

- It is trivial to verify that when working for *c**Δ*t*, we get the success probabilities:

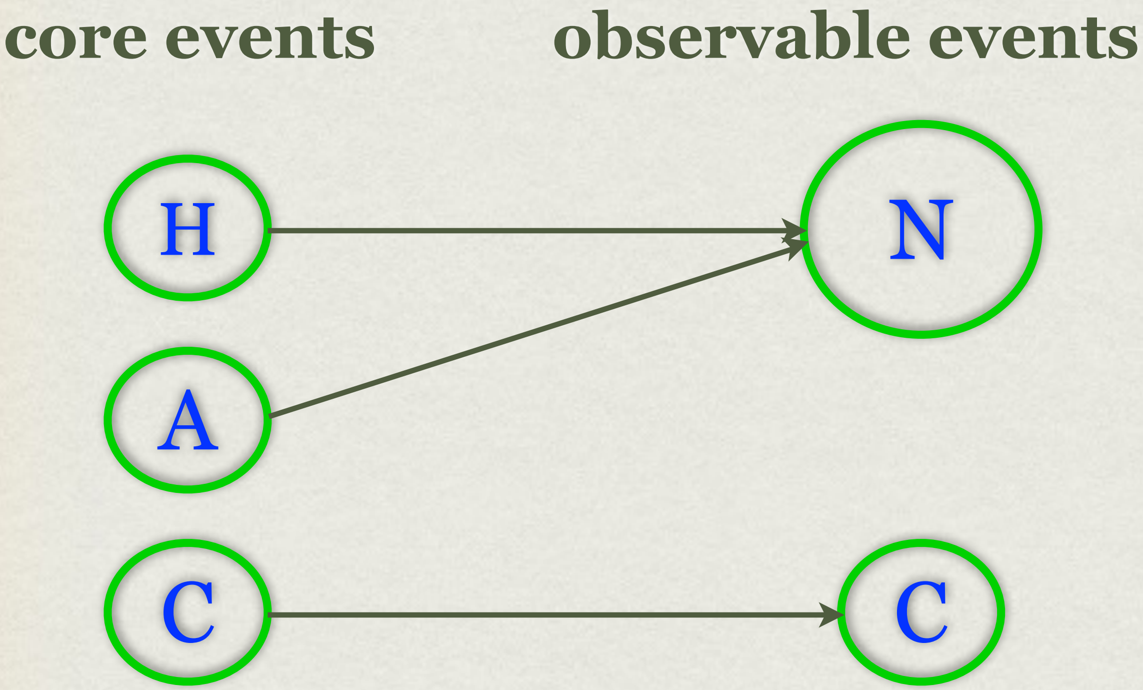
$$1-(1-\Pr[H])^{c}=1-(1-\tfrac{target}{2^{256}})^{\gamma c}$$

$$1-(1-\Pr[A])^{c}=1-(1-\tfrac{target}{2^{256}})^{\alpha c}$$

- So, we can use Pr[*H*] and Pr[*A*] to model the honest and attacking nodes computational power, respectively.

CHANNEL MODEL

- *Physical argument:* We shall assume Δt such small that $\Pr[H \cap A]$ can be neglected w.r.t. $\Pr[H]$ and $\Pr[A]$. Then we get the following model:



$$p = \Pr[H \mid N] = \frac{\Pr[H \cap N]}{\Pr[N]} = \frac{\Pr[H]}{\Pr[N]}$$

$$q = \Pr[A \mid N] = \frac{\Pr[A \cap N]}{\Pr[N]} = \frac{\Pr[A]}{\Pr[N]}$$

$$p + q \cong \frac{\Pr[N]}{\Pr[N]} = 1 \text{ and } \frac{q}{p} = \frac{\Pr[A]}{\Pr[H]}$$

WHO IS WHO?!

- It is important to understand that **even honest nodes cannot be sure** of which nodes are driven by attackers.
- So, the channel model that actually hides the intention of a new block - *up to a certain probability* - is quite accurate here.
    - Furthermore, from a mathematical viewpoint, it allows us to ground our reasoning considerably firmer.

EXPECTED TIME

- Let the honest nodes have just produced *z* blocks in the BlockChain.
  - The number of *time instants X* required for one block is given by a geometric distribution with probability Pr[*H*].
  - So E(*X*) = 1/Pr[*H*].
  - For *z* blocks, we get $E(X_1 + X_2 + \ldots + X_z) = z{*}E(X) = z/\Pr[H]$.
- So, we can **estimate** that *z*/Pr[*H*] *time instants* have already passed before the honest nodes have got those *z* blocks.

POISSON PHASE

- The expected number of attackers' blocks found in those time instants is $\boldsymbol{\lambda} = z*\Pr[A]/\Pr[H] = \boldsymbol{z*q/p}$ (*thanks to the channel model*).
  - Rigorously, we should also investigate time instants variance, since $z/\Pr[H]$ is just an expected value!
  - Otherwise, we get a kind of "expected probability" which is good for an overview, but it causes e.g. apparent antisymmetry when investigating $q \approx p$.
- The **particular no. of dishonest blocks** found meanwhile then follows the Poisson distribution:

$$\Pr[Y = k] = \boxed{e^{-\lambda}\frac{\lambda^k}{k!}}$$

GAMBLER'S RUIN

- *A gambler starts with a stake of size* s *and plays until their capital reaches the value* M *(gambler wins) or the value* 0 *(gambler is ruined).*
  - It is a kind of random walk in $\boldsymbol{R}^1$.
- Here, we study the probability the gambler is eventually ruined when playing against *infinitely rich* adversary. The **gambler is the set of honest nodes** here.
  - **Ruining the gambler is a necessary condition** for the attackers to win.
  - The *infinitely rich* adversary means there is no such *M* after which the attacking nodes would give it up.

GAMBLING PHASE

- Gambler wins a round with probability *p* and **looses with *q***.
  - Win increments, while **loss decrements** gambler's stake.
  - We need *p* + *q* = 1 which is roughly guaranteed by *the channel model* again.
- Let *q*(*z* - *k*) be the probability of gambler's ruin when starting with *s* = *z* - *k*. Assuming *p* > *q*, we have:

$$q(z-k) = \begin{cases} \lim\limits_{M\to\infty} \dfrac{\left(\frac{q}{p}\right)^{M} - \left(\frac{q}{p}\right)^{z-k}}{\left(\frac{q}{p}\right)^{M} - 1} = \left(\frac{q}{p}\right)^{z-k} & \text{if } z>k \\ 1 \text{ otherwise} \end{cases}$$

FINALLY

- Under a plausible assumption of SHA-256 results independence among the *Poisson and gambling phases*, we can directly multiply the respective probability distributions.
- Summing up for all possible attacking chain lengths *k* advances (while the honest group has made *z* honest blocks), gives the upper bound

$$Q(p,q,z) \leq \sum_{k=0}^{\infty} e^{-\lambda} \frac{\lambda^k}{k!} \cdot \begin{cases} \left(\frac{q}{p}\right)^{z-k} & \text{if } z>k \\ 1 \text{ otherwise} \end{cases}$$

$$\lambda = z\frac{q}{p}$$

Q.E.D.

COMPLEMENT EQ.

- To evaluate the formula programmatically, we can use the complement probability to get a finite number of summands.

$$Q(p,q,z) \leq 1 - \sum_{k=0}^{z-1} e^{-\lambda} \frac{\lambda^k}{k!} \left(1 - \left(\frac{q}{p} \right)^{z-k} \right)$$

$$\lambda = z \frac{q}{p}$$

attackers have already prepared *k*<z blocks

no catch up for the remaining *z-k* blks

PUT IT ANOTHER WAY

$$\lim_{N\to\infty}\sum_{k=0}^{N} e^{-\lambda}\frac{\lambda^k}{k!}\cdot\begin{cases}\left(\frac{q}{p}\right)^{z-k} & \text{if } k<z\\ 1 \text{ otherwise}\end{cases}$$

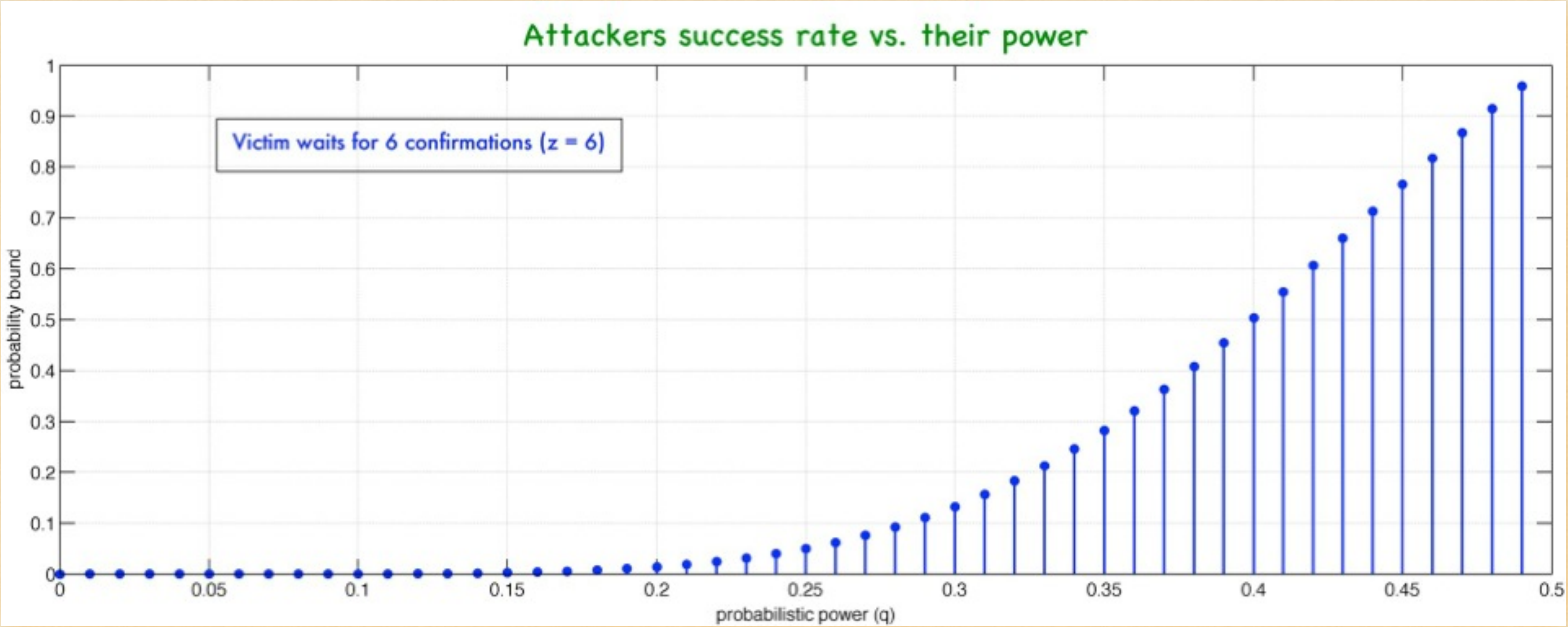
$$=\lim_{N\to\infty}\left[\left(\sum_{k=0}^{N} e^{-\lambda}\frac{\lambda^k}{k!}\right)-\left(\sum_{k=0}^{z-1} e^{-\lambda}\frac{\lambda^k}{k!}\right)+\left(\sum_{k=0}^{z-1} e^{-\lambda}\frac{\lambda^k}{k!}\left(\frac{q}{p}\right)^{z-k}\right)\right]$$

$$=1-\left(\sum_{k=0}^{z-1} e^{-\lambda}\frac{\lambda^k}{k!}-\sum_{k=0}^{z-1} e^{-\lambda}\frac{\lambda^k}{k!}\left(\frac{q}{p}\right)^{z-k}\right)$$

$$=1-\sum_{k=0}^{z-1} e^{-\lambda}\frac{\lambda^k}{k!}\left(1-\left(\frac{q}{p}\right)^{z-k}\right)$$

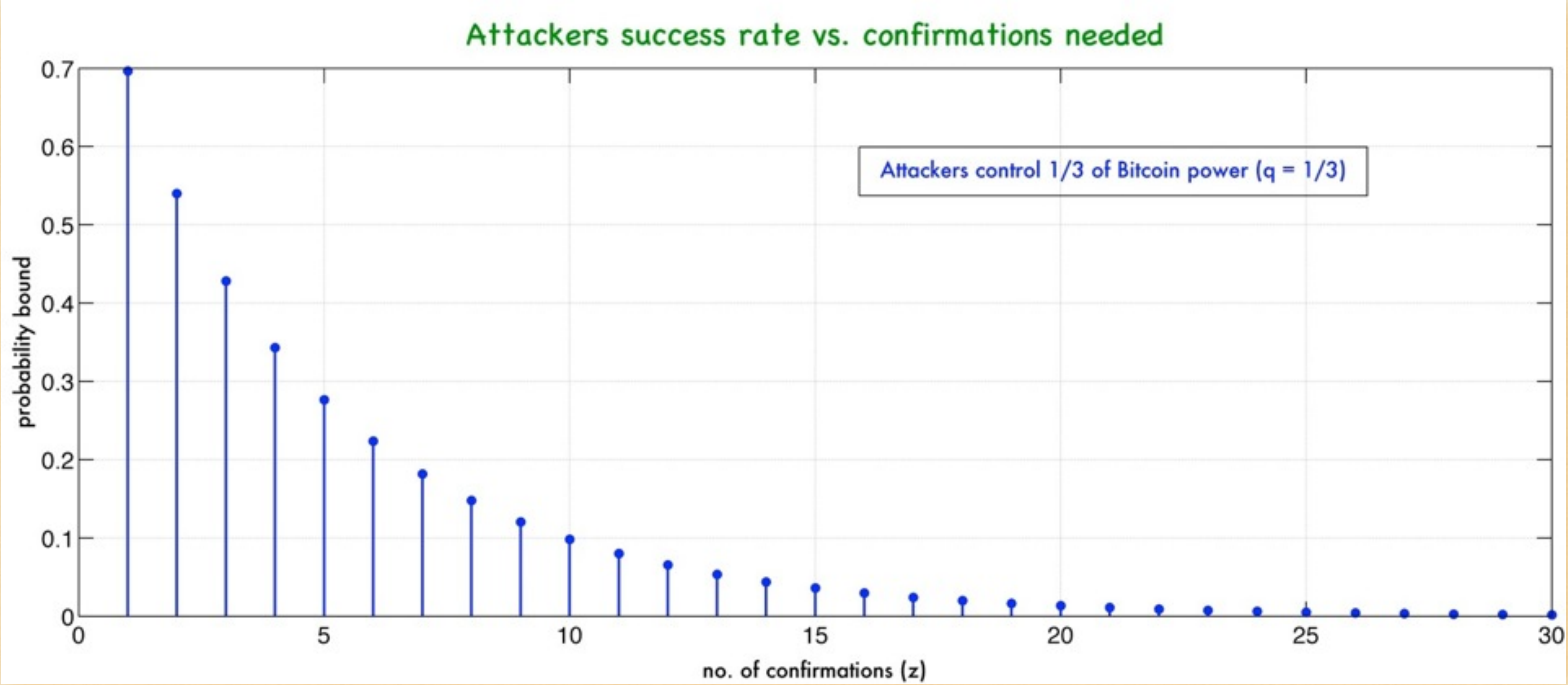
ATTACK PLANNING

- Or, how much of Bitcoin computing power do attackers need to control for a particular chance to win the double spending attack.

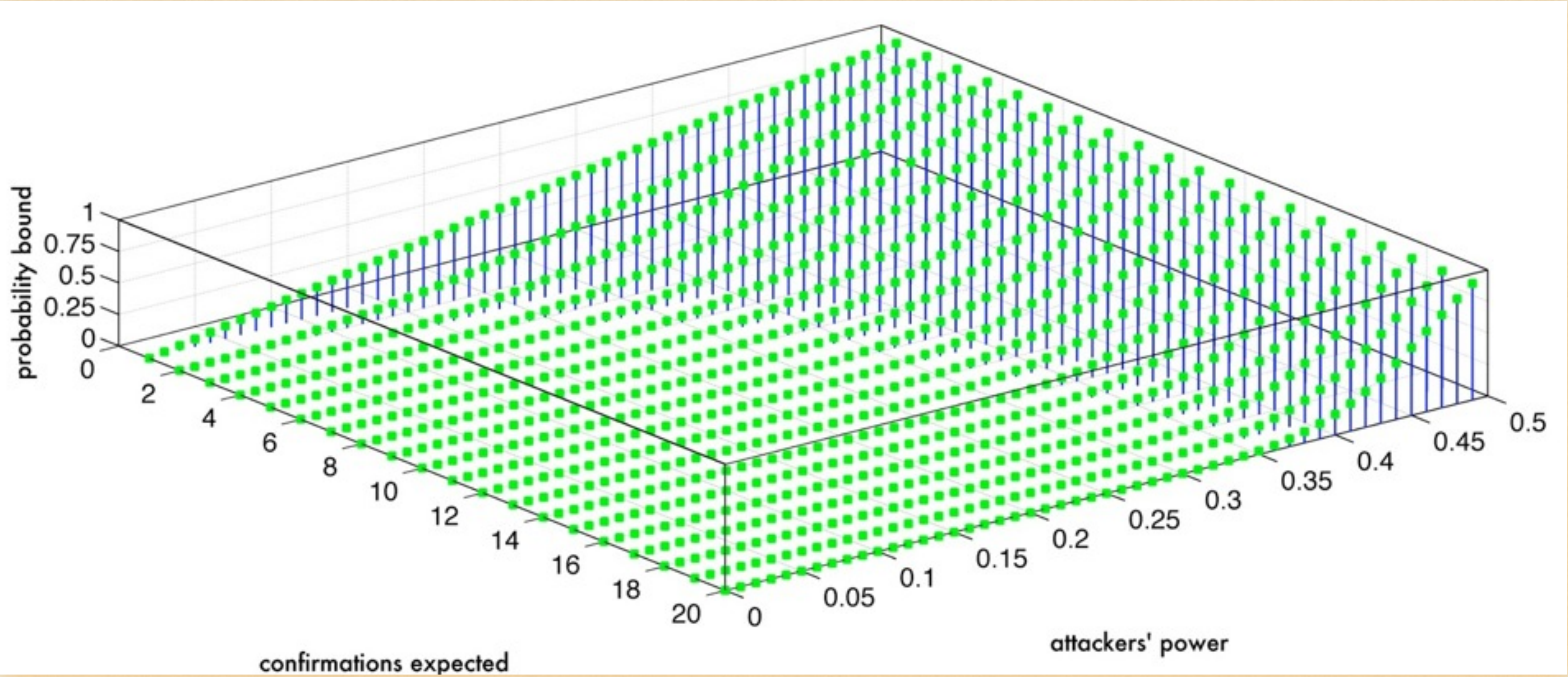


ENOUGH IS ENOUGH

- Or, how many confirmations shall we require before taking the transaction as granted, provided we assume attackers own at most 1/3 of the total Bitcoin power.



VIEW TO A HACK



BE AWARE

- Despite our effort, we have in fact investigated just one out of many attacking scenarios.
  - It **suffices to understand** how the Bitcoin voting should work.
  - It is, however, **not enough to say the Bitcoin is secure**.
- The Bitcoin distributed system shall be further analyzed to see whether there are some "shortcuts" to circumvent the voting mechanism with much less power.
  - For instance, attackers can - besides preparing the alternate chain - try to fragment the honest nodes effort by inducing a creation of several slower-growing parallel chains. It is an open question to check how it would help.

HIDDEN ADVANTAGE

- Furthermore, there is an **intrinsic advantage of dishonest nodes** over the honest ones.
    - Attackers can follow certain strategy that is beyond the scope of the *original Bitcoin node policy and topology*.
    - The honest ones, on the other hand, follow just the rules of the symmetric distributed system. Especially, they will not (and cannot!) form a special coalition against the attackers.

FOR EXAMPLE

- Should the bad ones be some blocks behind the honests, they nevertheless keep trying to find another blocks and to possibly ruin the gambler (the honest ones) some day.
- On the other hand, should the good ones loose the leading position even once, they will be willing to faithfully join the attackers chain instead!

FINAL REMARKS

- Despite certain effort, we can hardly say we have covered all the Bitcoin security.

- We have reviewed the most important cryptographic mechanisms, while e.g. formally deriving the arguments behind the BlockChain voting mechanism that were *just stated* in the original paper by Nakamoto.

- Still, a lot of things deserve further attention. For instance:

  – Malware attacks on the Wallet

  – Exploits in *transaction scripts*

  – Information propagation in the Bitcoin network and so-called *fast transactions* that are faithfully based on transaction broadcasts only (not waiting for BlockChain confirmations)

  – Hidden assumptions on network security (e.g. MITM in various places)

  – Collusive mining pools and other unfair tactics resulting into either direct fraud or at least Pr[H] perturbations (possibly invalidating security proofs)

CONCLUSION

- From academic perspective, Bitcoin is a valuable inter-science experiment that will for sure motivate a lot of interesting research.
- From a practical viewpoint, well... it is just here and we have to face it.
    - Something can be predicted by simply looking at online banking systems history - e.g. malware attacks on wallets.
    - Other parts are yet to be analyzed and it is really hard to say now even whether (serious) academic research will precede real attacks or vice versa.

Some people perceive the Bitcoin like this...

ACKNOWLEDGEMENTS

– *Practical Bitcoin experiments were carried in our lab with a kind cooperation of Ondřej Pokorný.*

REFERENCES

1. Androulaki, E., Karame, G.-O., Roeschlin, M., Scherer, T., and Capkun, S.: *Evaluating User Privacy in Bitcoin*, In Proc. of Financial Cryptography and Data Security, LNCS Vol. 7859, pp. 34-51, 2013

2. *Bitcoin wiki*, https://en.bitcoin.it/wiki/Main_Page

3. Clark, C.: *Bitcoin Internals - A Technical Guide to Bitcoin*, Kindle edition, Amazon Digital Services, Inc., 2013

4. Decker, C. and Wattenhofer, R.: *Information Propagation in the Bitcoin Network*, 13th IEEE International Conference on Peer-to-Peer Computing, 2013

5. Eyal, I. and Sirer, E.-G.: *Majority is not Enough: Bitcoin Mining is Vulnerable*, arXiv: 1311.0243v5, November 15, 2013

6. Hamacher, K. and Katzenbeisser, S.: *Bitcoin - An Analysis*, 28th Chaos Communication Congress, 2011

7. Karame, G.-O., Androulaki, E., and Capkun, S.: *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*, In Proc. of Conference on Computer and Communication Security, 2012

8. Nakamoto, S.: *Bitcoin: A Peer-to-Peer Electronic Cash System*

9. *Wikipedia - The Free Encyclopedia*, http://www.wikipedia.org