Crypto Currencies
P2P Payment
Value Transfer Networks

Nicolas T. Courtois

- **U**niversity **C**ollege **L**ondon, UK

UCL Bitcoin Seminar

UCL crypto currency seminar and special interest group

every **Thur 12h00-14h00 -**
room and exact hour varies

public web page: www.want2pay.com

Introducing Bitcoin

Bitcoin In A Nutshell

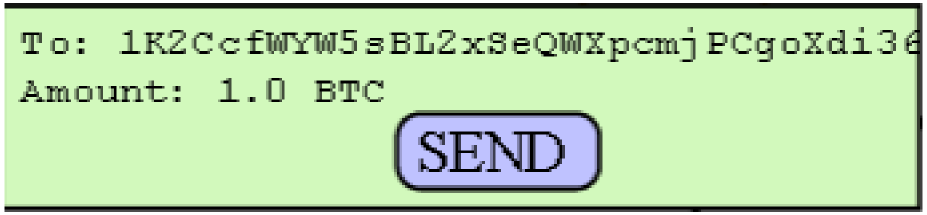
- bitocoins are cryptographic tokens
  - stored by people on their PCs or mobile phones
- ownership is achieved through digital signatures:
  - you have a certain cryptographic key, you have the money.
  - publicly verifiable, only one entity can sign

- consensus-driven, a distributed system which has no central authority
  - but I will not claim it is decentralized, this is simply not true!
  - a major innovation is that financial transactions CAN be executed and policed without trusted authorities. Bitcoin is a sort of financial cooperative or a distributed business.
- based on self-interest:
  - a group of some 100 K people called bitcoin miners own the bitcoin “infrastructure” which has costed about 0.5-1 billion dollars (estimation)
  - they make money from newly created bitcoins and fees
  - at the same time they approve and check the transactions.
  - a distributed electronic notary system

Two Key Concepts

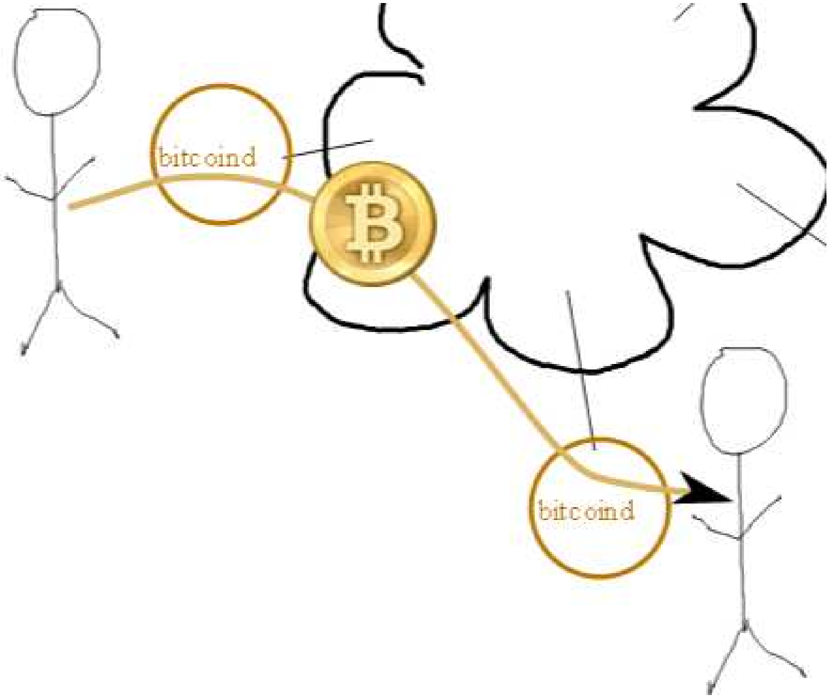
- initially money are attributed through **Proof Of Work (POW)** to one public key A
  - to earn bitcoins one has to “work” (hashing) and consume energy (pay for electricity)
  - in order to cheat one needs to work even much more (be more powerful than the whole network, for a short while)
- money transfer from public key A to public key B:
  - **like signing a transfer in front of one notary which confirms the signature**,
  - multiple confirmations: another notary will re-confirm it, then another, etc…
  - we do NOT need to assume that ALL these notaries are honest.
    - at the end it becomes too costly to cheat

Money Transfer

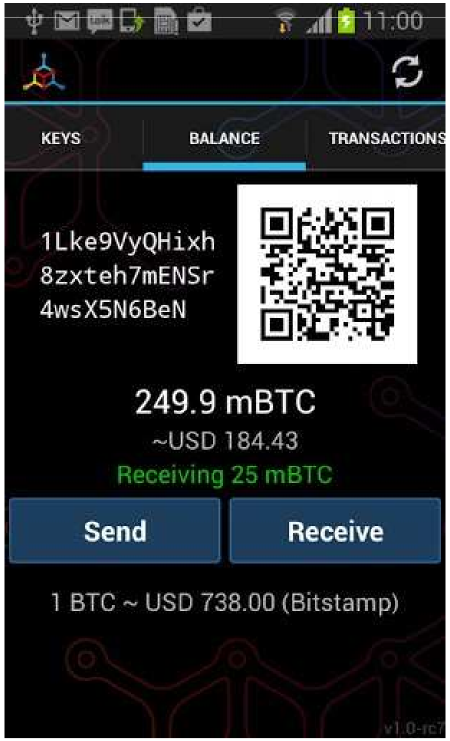


To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36

Amount: 1.0 BTC



In Practice



1Lke9VyQHixh8zxteh7mENSr4wsX5N6BeN

249.9 mBTC

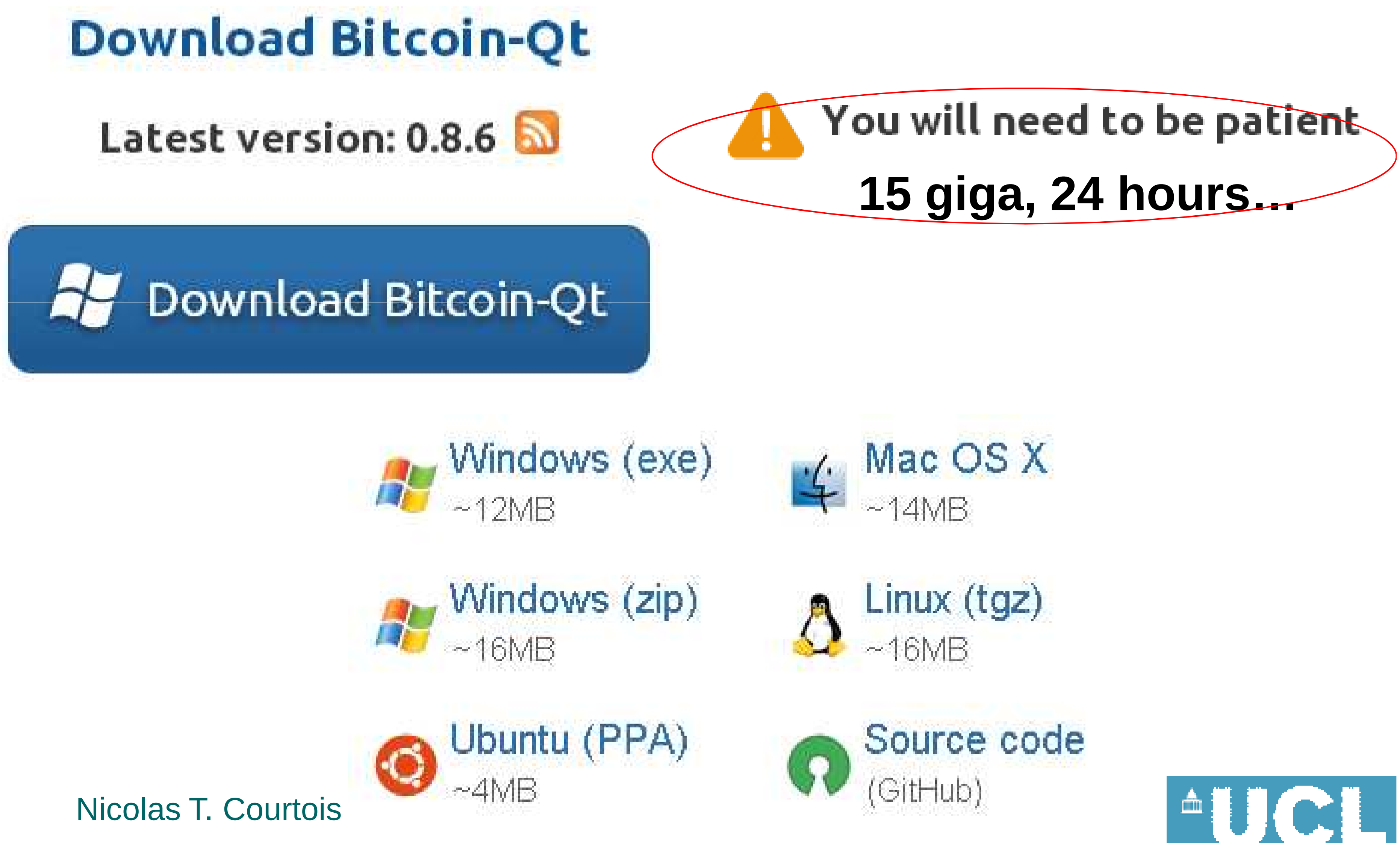
~USD 184.43

Receiving 25 mBTC

1 BTC ~ USD 738.00 (Bitstamp)

Full P2P Client

http://bitcoin.org/en/download



Download Bitcoin-Qt

Latest version: 0.8.6

⚠ You will need to be patient

15 giga, 24 hours…

Windows (exe)
~12MB

Mac OS X
~14MB

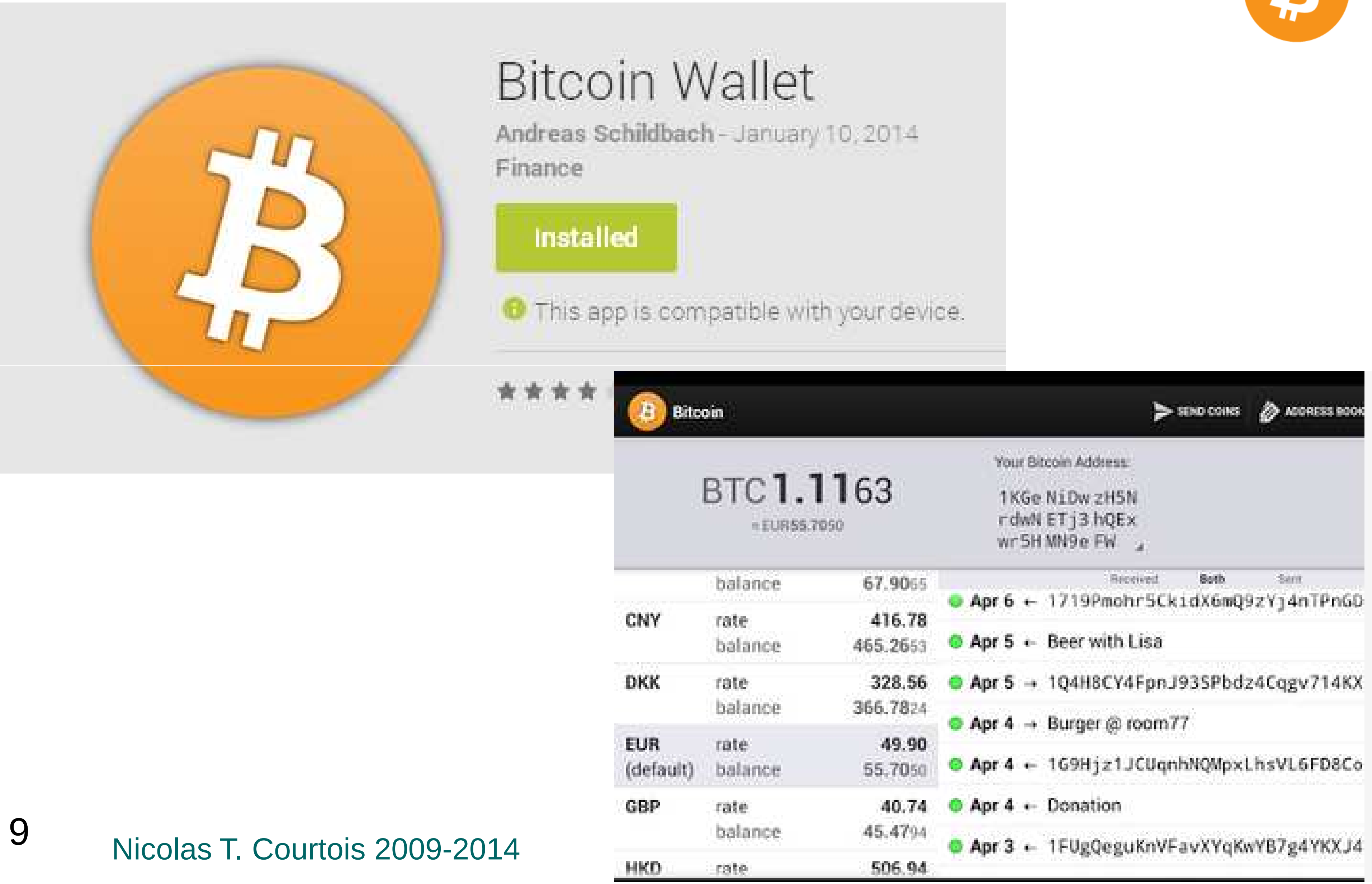
Windows (zip)
~16MB

Linux (tgz)
~16MB

Ubuntu (PPA)
~4MB

Source code
(GitHub)

Mobile Apps - Android



Bitcoin Wallet

Andreas Schildbach - January 10, 2014

Finance

This app is compatible with your device.

BTC 1.1163

≈ EUR55.7050

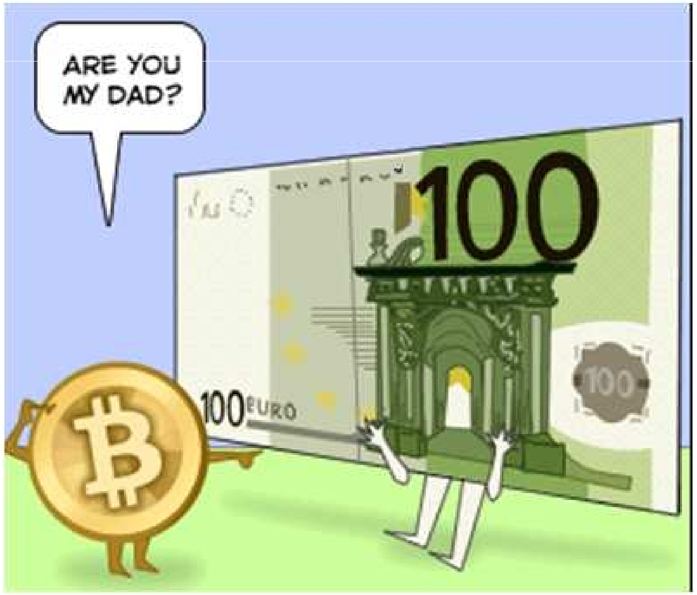
Your Bitcoin Address:

1KGe NiDw zH5N
rdwN ETj3 hQEx
wr5H MN9e FW

	balance	67.9065
CNY	rate	416.78
	balance	465.2653
DKK	rate	328.56
	balance	366.7824
EUR (default)	rate	49.90
	balance	55.7050
GBP	rate	40.74
	balance	45.4794
HKD	rate	506.94

● Apr 6	←	1719PmohrSCkidX6mQ9zYj4nTPnGD
● Apr 5	←	Beer with Lisa
● Apr 5	→	1Q4H8CY4FpnJ93SPbdz4Cqgv714KX
● Apr 4	→	Burger @ room77
● Apr 4	←	1G9Hjz1JCUqnhNQMpxLhsVL6FD8Co
● Apr 4	←	Donation
● Apr 3	←	1FUgQeguKnVFavXYqKwYB7g4YKXJ4

Is Bitcoin Money?



© 2014 Geek Culture

Is Bitcoin Money?

- We will NOT claim it has all the characteristics of money.
  - it definitely has some!

Two Main Functions of Money

1. Store Value
2. Allow Payment ₿

CAN BE IMPLEMENTED DIFFERENTLY!

SEPARATION IS NOT FORBIDDEN

Bitcoin

Bitcoin =

… the most popular peer-to-peer payment and virtual currency system as of today

belongs to no one, anarchy

~~UK Payments~~
~~Administration~~
=>

Crypto Currencies

Bitcoin

Decentralized peer to peer payment system which works as currency:
=> has units of value which can be exchanged for “real money”. Currently 1BTC= 600 USD.

Based on cryptography and network effects.

Anarchy, not supported by any government and not issued by any bank.

“Play money”, imperfect system.

*Disruption?

Disruptive Technology:

def:

Allows to do things which just could not be done before…

Krugman

- Bitcoin is …
  - just one of possible ways
    to pay electronically [irony ☺]

– Paul Krugman,
Nobel price in economics

More Krugman!

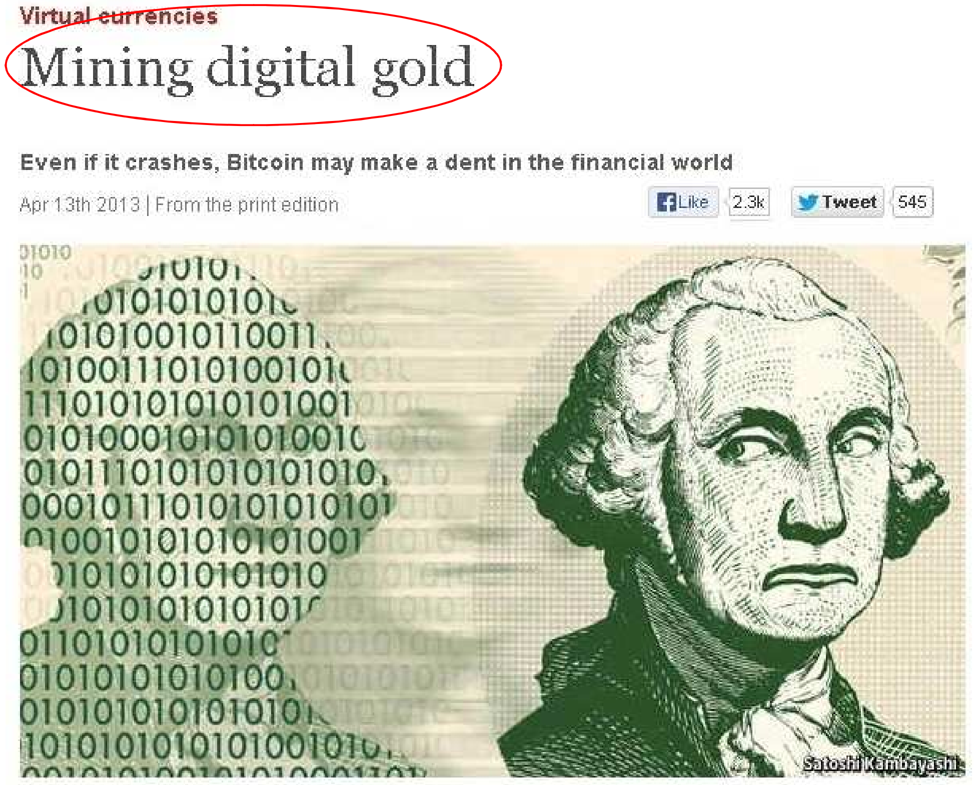
- Bitcoin is …
  - “the anti-social network”

– Paul Krugman,
Nobel price in economics

13 April 2013

HOWEVER

The Economist



Virtual currencies

Mining digital gold

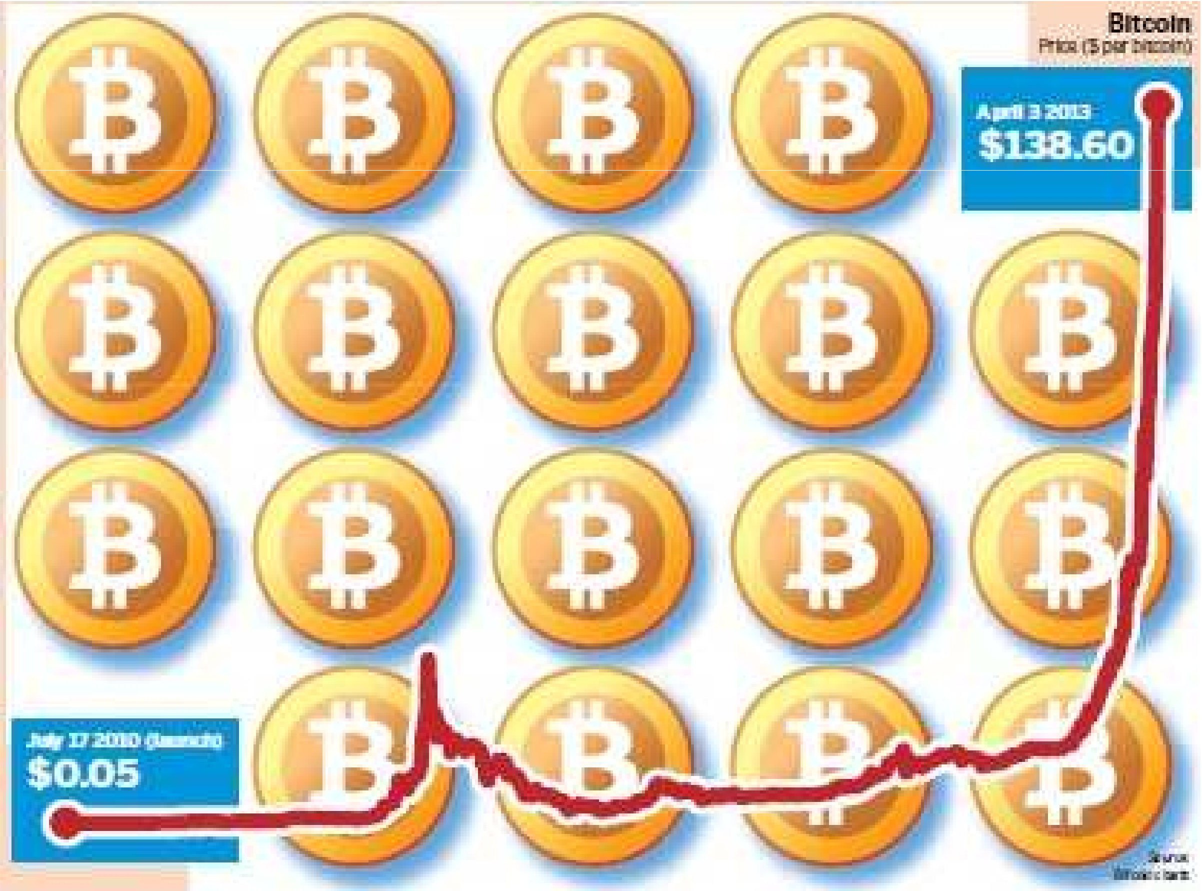
Even if it crashes, Bitcoin may make a dent in the financial world

Apr 13th 2013 | From the print edition

FINANCIAL TIMES

USA Thursday April 4 2013

Buying frenzy sends virtual currency on way to becoming next bubble



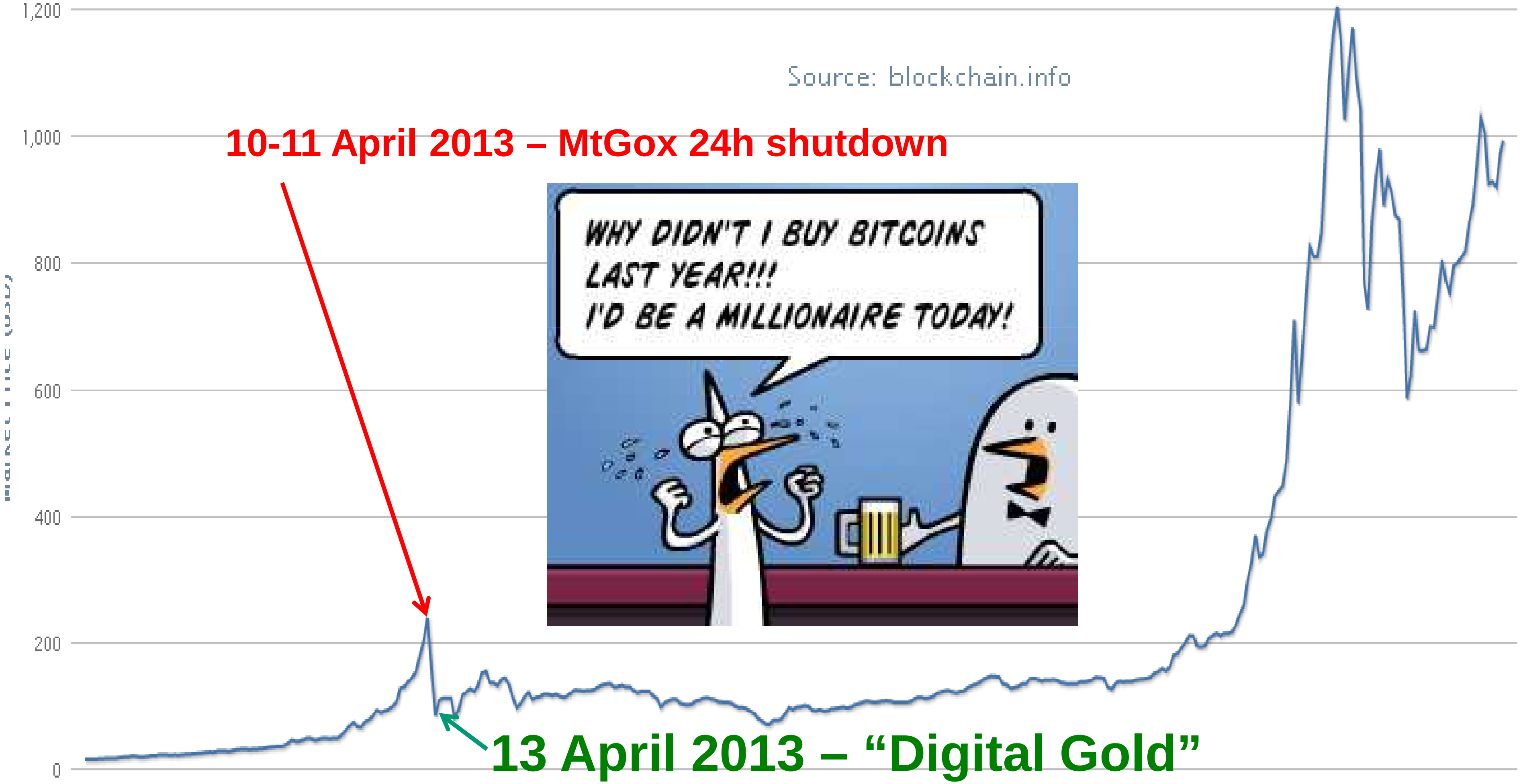
Source: Bitcoincharts

bubble?

they have seen nothing yet!

Jan 2013-Jan 2014

14 => 1000 USD

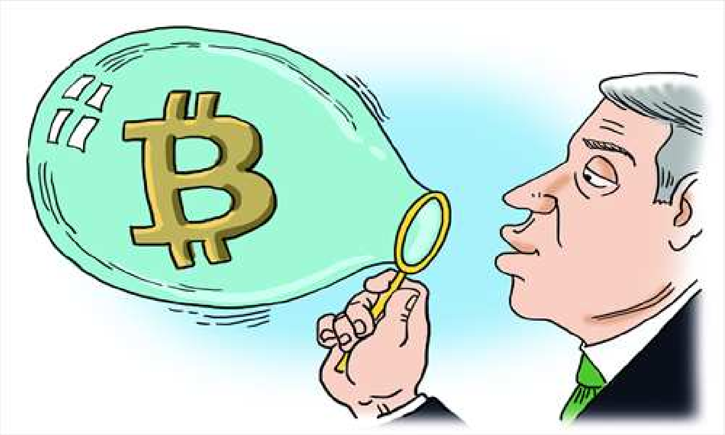


Source: blockchain.info

10-11 April 2013 – MtGox 24h shutdown

13 April 2013 – "Digital Gold"
The Economist

Another Nobel Price:

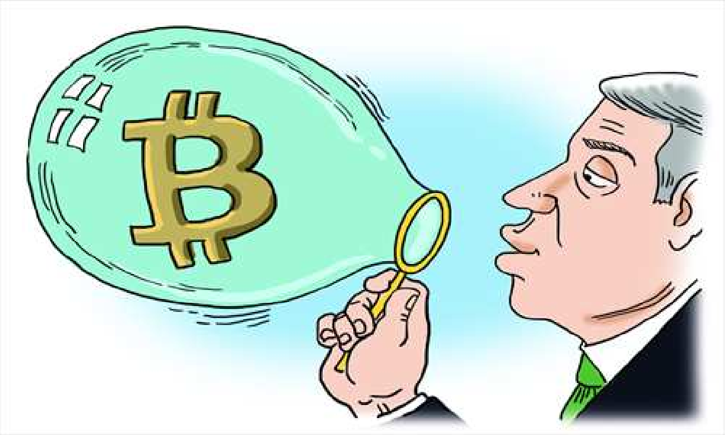


In Davos Jan 2014:

"It is a bubble,
there is no question about it.
… It's just a amazing example of a bubble."

– Robert Shiller, Nobel price in economics, awarded specifically for work on asset bubbles.

“Bots Caused Bitcoin Bubble”



Anonymously published Willy Report:

- algorithms, named Markus and Willy, bought up 650,000 bitcoins in the dying days of the MtGox exchange, causing the price of bitcoin to soar above $1,000.
- “there is a ton of evidence to suggest that all of these accounts were controlled by MtGox themselves“
- “so if you were wondering how bitcoin suddenly appreciated in value by a factor of 10 within the span of one month, well, this may be why."
- …also claimed to be bought with customer money

http://www.ibtimes.co.uk/cryptocurrency-news-round-mtgox-bots-caused-bitcoin-bubble-darkcoin-dives-1450415

Miracle Of Bitcoin

Removes two pillars of money:

- “trust”

  => Peer 2 Peer self-regulation based on self-interest?

- legal/government protection and policing

  => anarchy!

*Anarchy!

- Until recently, we’ve needed central bodies – banks, stock markets, governments, police forces – to settle vital questions.
  - Who owns this money?
  - Who controls this company?
  - Who has the right to vote in this election?
- Now we have a small piece of pure, incorruptible mathematics enshrined in computer code that will allow people to solve the thorniest problems without reference to “the authorities”.

http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html
[11 June 2014]

Is Bitcoin Money?

A Currency?

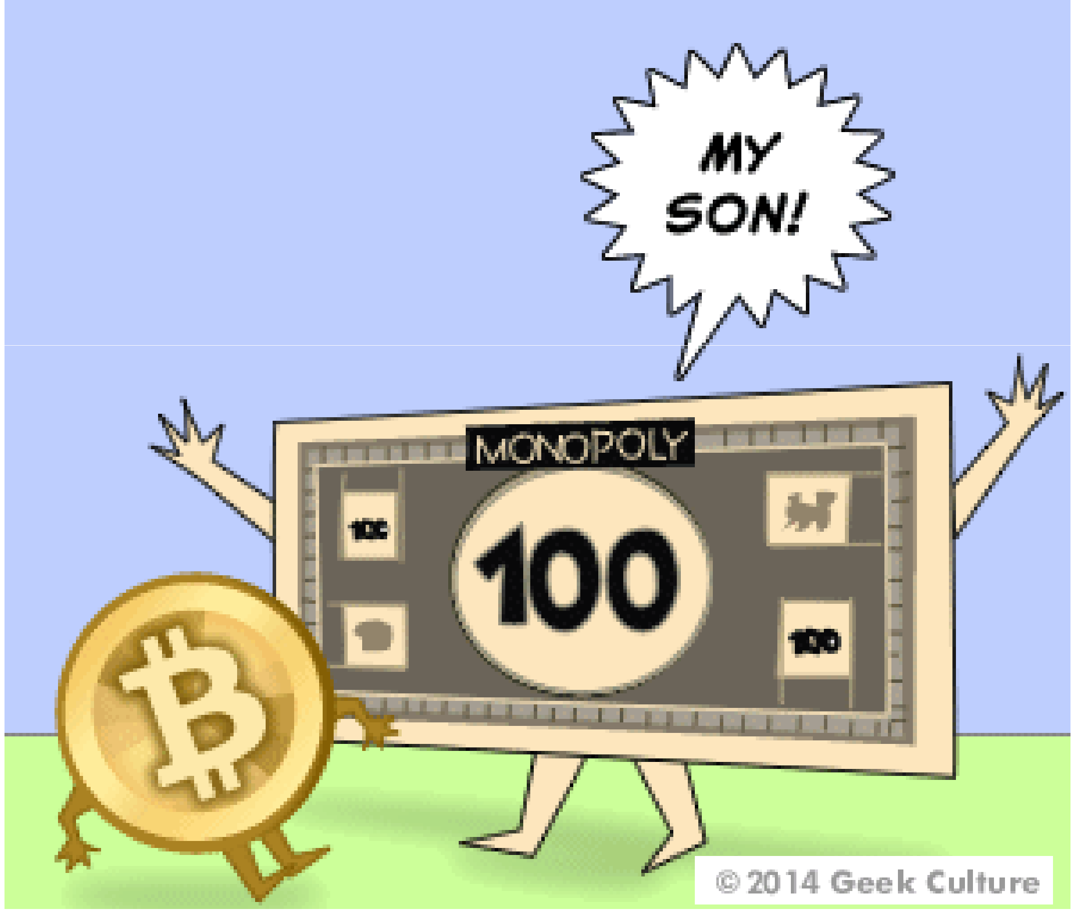
SEE Part 1 of these slides.

Are They Crazy?

Anything can be “money”
if sufficiently many people accept it…

Play Money?

A distinction play vs. real money has almost disappeared recently.

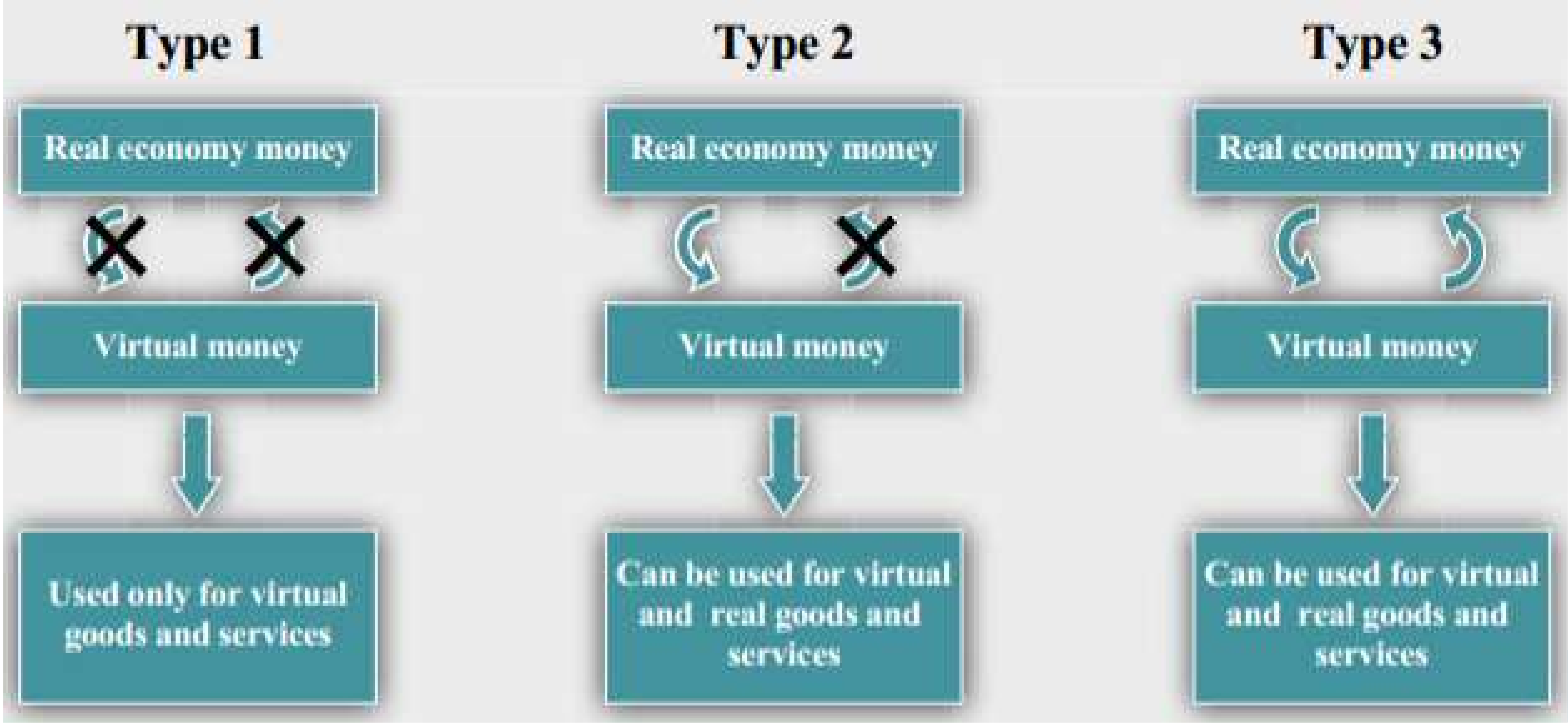


Types of “Virtual Money”

Source: ECB report, 10/2012

http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

cf. Oyster…


Type 1
Real economy money
Virtual money
Used only for virtual goods and services
Type 2
Real economy money
Virtual money
Can be used for virtual and real goods and services
Type 3
Real economy money
Virtual money
Can be used for virtual and real goods and services

Bitcoin!

A payment system in which

- it is THE PAYER who initiates the transaction
- controls the amount being paid
- money and payments are stored outside of the banking system [erodes the dominant position of banks]
- money cannot be confiscated [cf. Cyprus banks].
- it challenges fractional reserve banking [new!]
- it forces finance to become more “transparent”

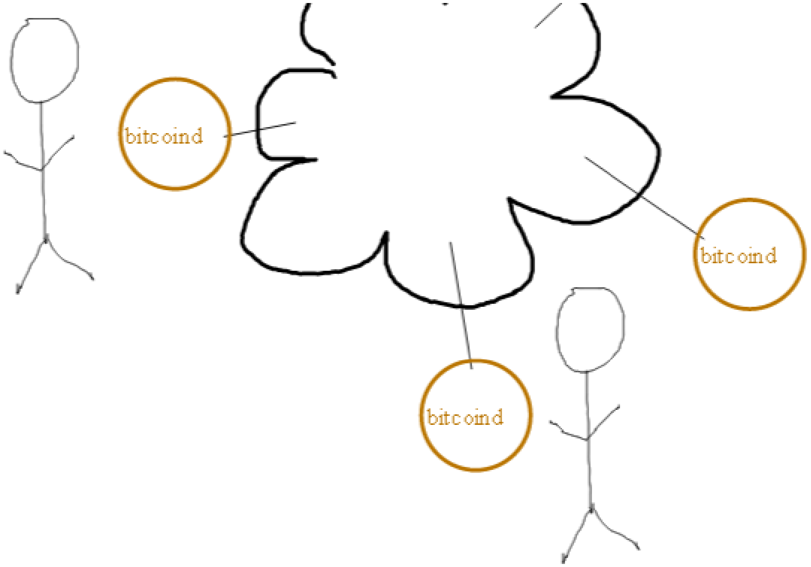
P2P Payment

Bitcoin Network

- Peer to peer, decentralized, no central authority, one ASIC one vote,

  => no third party risk [no need to trust the banker!]

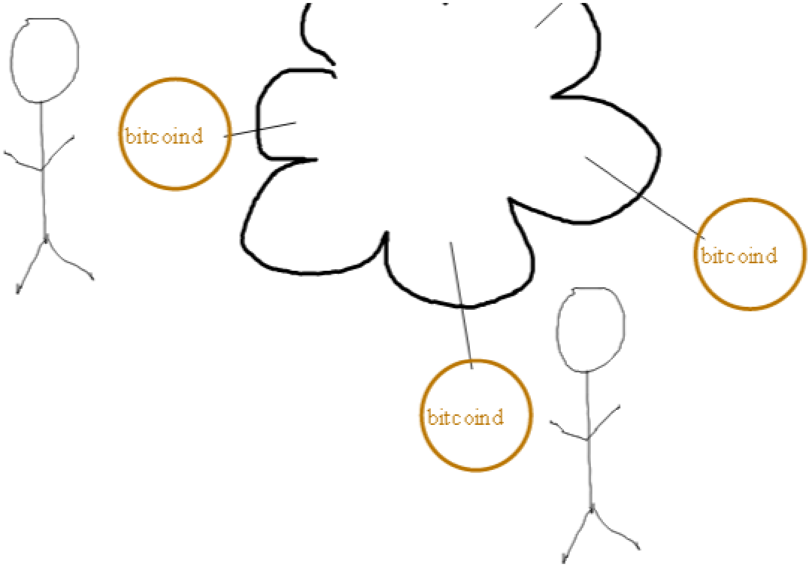
- Knows no limits, borders, laws, etc…
  - Computers connected into a P2P network…
  - Every transaction can be downloaded by anyone…



1 client app

Bitcoin

- A Value Transfer Network
  - term proposed by a Wall Street lawyer Maese.
  -



More Than a Network

- Also a community:
  - adopters, developers, miners, speculators, etc…
- Upgrade the software, change the spec:
  - people vote with their feet
  - bitcoin belongs to no one

Network Properties

Satoshi original idea [cf. Sect. 5 in his paper]:

- homogenous nodes: they do the same job
  - everybody participates equally
  - everybody is mining
  - a random graph
- it appears that the current network resembles "a random graph"

The Reality is VERY Different!

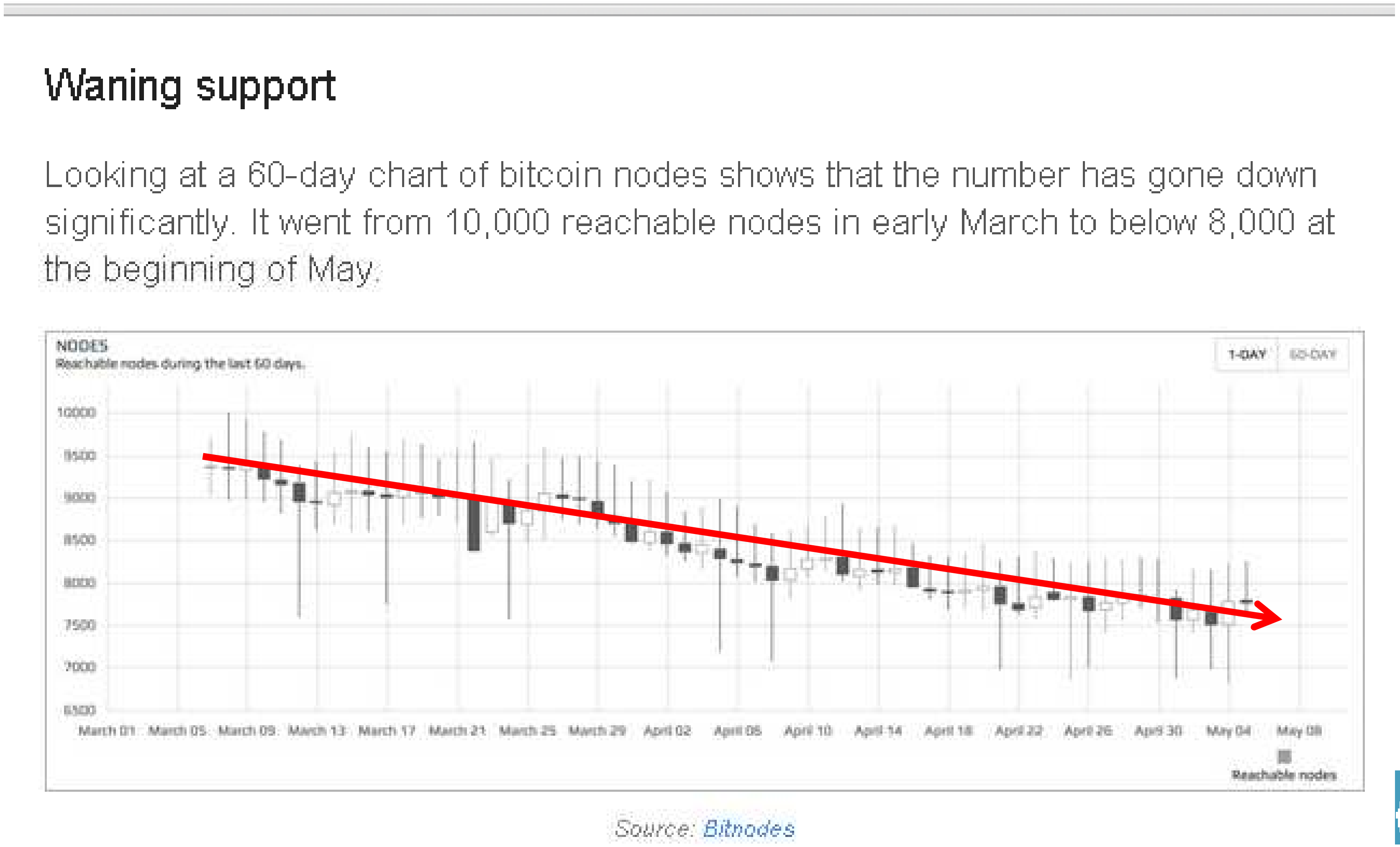
In violation of the original idea of Satoshi Bitcoin network has now 3 sorts of VERY DIFFERENT ENTITIES

- only “rich people” are mining
  - upfront investment of >3000 USD.
  - 100K active miners as of today?
    - but NOT running network nodes, mining is highly centralized, see pools
- some “full nodes”: they trust no one
  - Satoshi client a.k.a. bitcoind, version 0.9.X. for PC,
  - 15 Gbytes, takes 1 day to synchronize, CPU/HDD load
    - only some 13 K out of 60 K accept incoming connections (4/2014)
    - panic in May 2014: declining, less than 8,000 peers online
- many nodes do minimal work and minimal storage, they need to trust some other network nodes

*Panic – May 2014

- # active nodes << #miners
- 8K << 100K

www.coindesk.com/bitcoin-nodes-need/



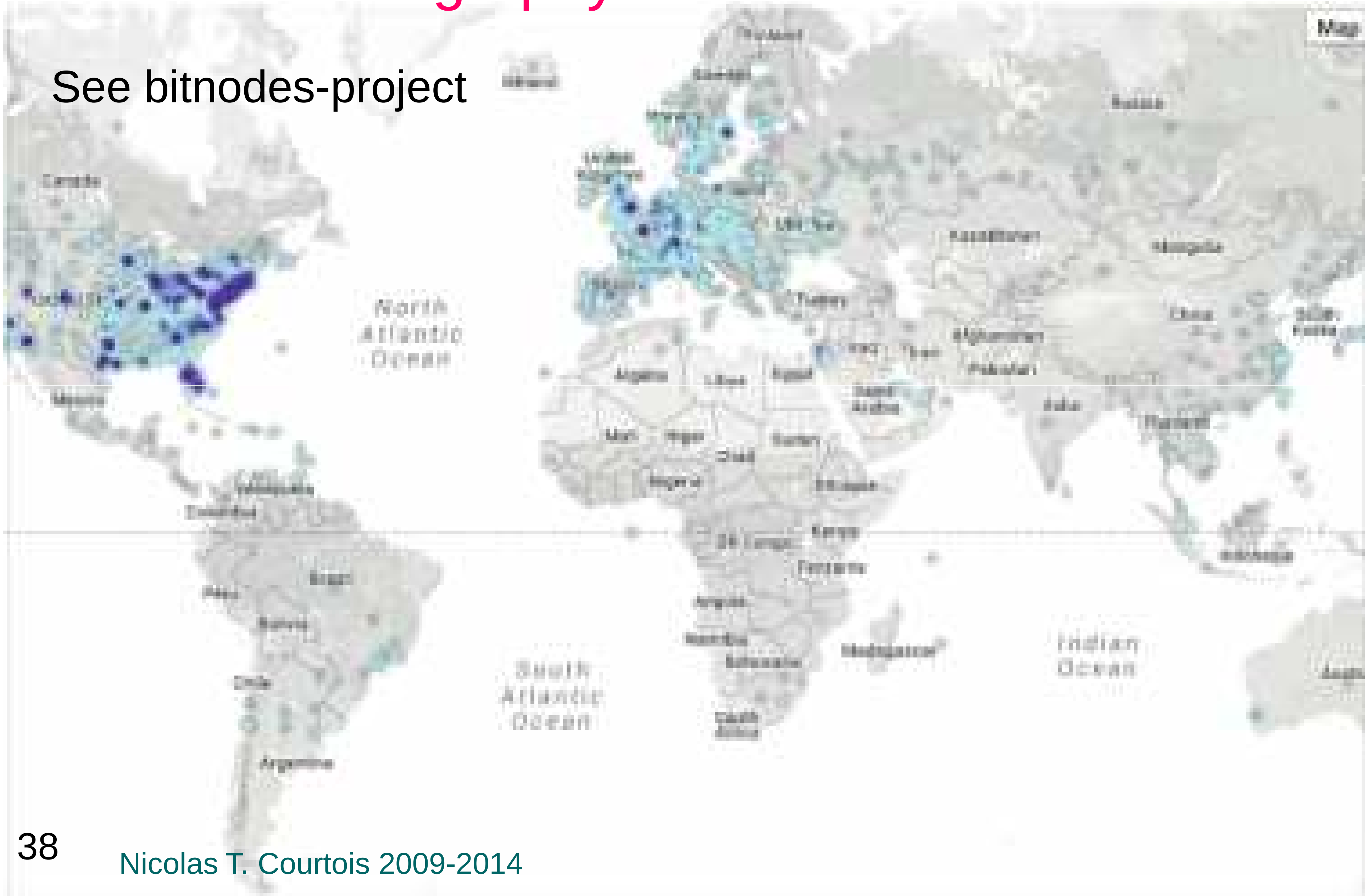
Waning support

Looking at a 60-day chart of bitcoin nodes shows that the number has gone down significantly. It went from 10,000 reachable nodes in early March to below 8,000 at the beginning of May.

Source: Bitnodes

Geography – Peer Network

See bitnodes-project



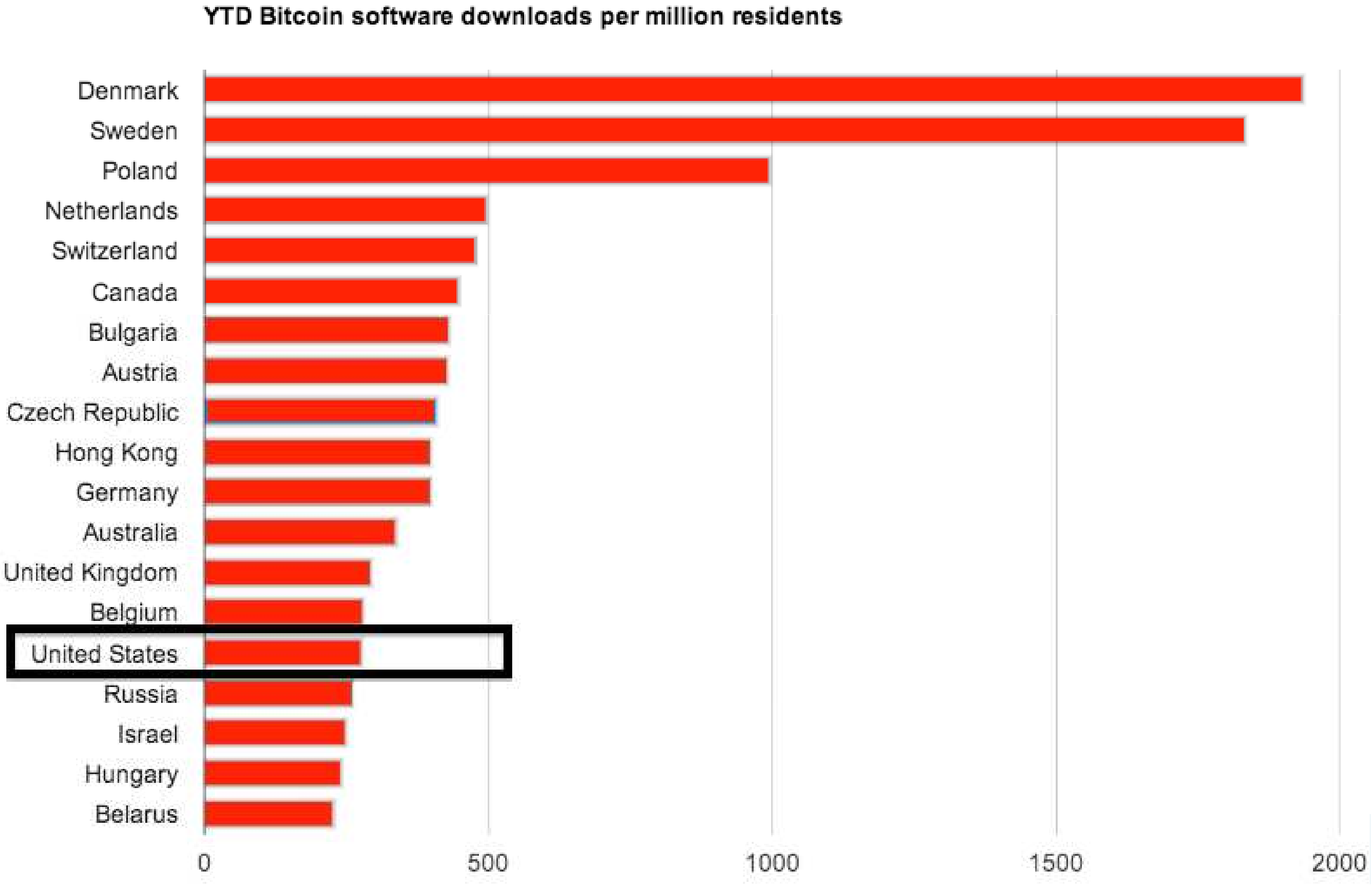
*Scalability Issues

- Current bitcoin processes only 0.7 transactions per second.
  - VISA processes 2000 transactions per second.
  - YES, even at this scale of 2000 tx/s bitcoin would theoretically work: each node receiving ALL new transactions would be like 1Mbit/second bandwidth.

- Limit on the size of one block = 1 Mb currently.
  - this can only accommodate 7 tr/sec
  - we are VERY close to exceed that, maybe in 6 months…

Bitcoin Downloads per Capita

http://www.businessinsider.com/bitcoin-is-going-to-take-off--just-probably-not-thanks-to-anyone-you-know-2014-6

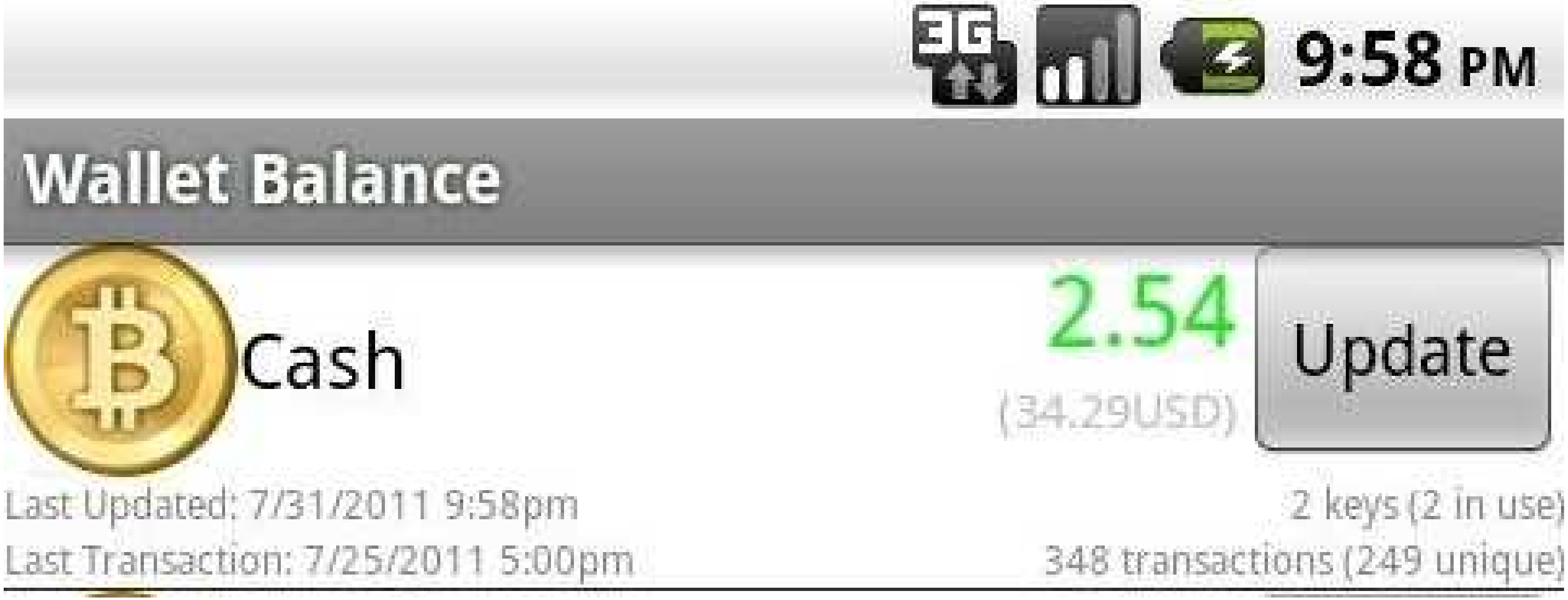


Key Properties of Bitcoin

- Consensus-driven
  - consensus about the past history[blockchain]
  - consensus about the future[software spec]
- Pseudonymous, NOT anonymous
- Ledger-based. Ledger is entirely public.
- Notion of account:
  - has a balance in BTC.
- Wallet:
  - computer file which stores "the money".

Wallets

- Wallet: file which stores your “money".
- A Bitcoin client App
  is also called a wallet



Wallet Balance

Cash

2.54

(34.29USD)

Update

Last Updated: 7/31/2011 9:58pm

Last Transaction: 7/25/2011 5:00pm

2 keys (2 in use)

348 transactions (249 unique)

Wallets == Bitcoin client Apps

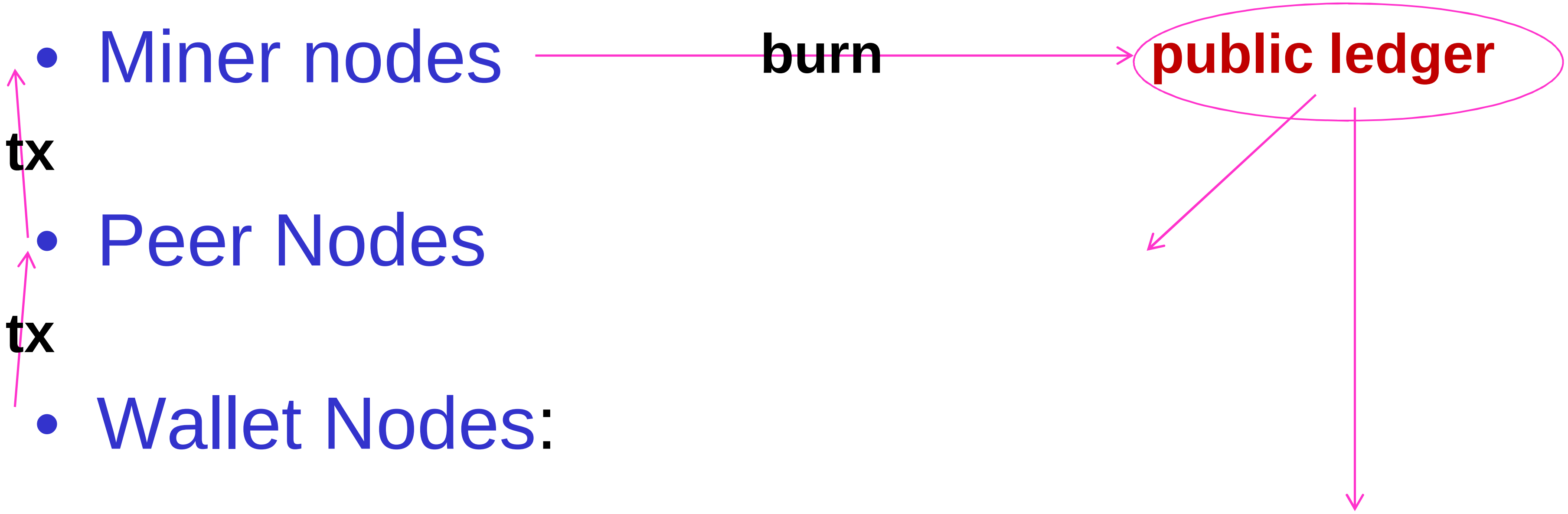
- Major types:
  1. Bitcoin Satoshi Core Client = Decent PC, full P2P node, stores full history - 15 Gb, trusts no one.
  2. Mobile apps: trust and rely on servers for DB and authenticity; but stores money locally.
  3. Cloud apps: all is stored in the cloud!
  4. Offline systems: protect your assets from cybercriminals
  5. Combined: multi-signature, THE BEST!

Further Separation?

It is possible to almost totally separate:

- Miner nodes
  - Hashing with public keys
- Peer Nodes
  - Relay and store transactions and blocks
- Wallet Nodes:
  - Store and release funds,
  - Focus on management of private keys, master keys etc etc.

Tx LifeCycle



- Miner nodes

tx

- Peer Nodes

tx

- Wallet Nodes:

burn

public ledger

*Why Separation

Separation makes a lot of sense in security engineering:

Principle of Separation of Privileges [Saltzer and Schroeder 1975]

Split software into pieces with limited privileges! Very common in software engineering:

- creating a child process,
- dropping privileges

=> A successful exploit against the larger program will gain minimal access.

Digital Currency

Digital Currency

1. Sth. that we know… String of Bits.

   + additional layers of security:

2. Sth that we can do (capability): BETTER.
   - can be used many times without loss of confidentiality…
   - in bitcoin bank account = a certain private ECDSA key…

=>PK-based Currency,
an important modern application of Digital Signatures!

Main Problem:

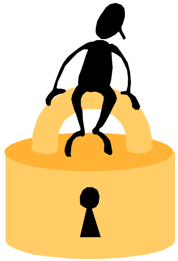
This capability can be "spent twice".

Avoiding this "Double Spending" is the main problem when designing a digital currency system.

NOT yet solved in a satisfactory way, instability, slow transactions, more about this later.

Cf. Nicolas Courtois: On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies http://arxiv.org/abs/1405.0534

Crypto



**Crypto Citations

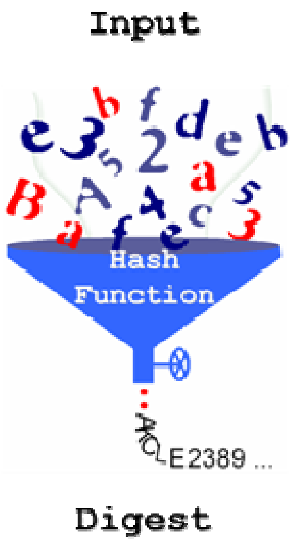
About Bitcoin:

- Security depends on maths, not people.
- The accuracy of past transactions is guaranteed by cryptography, which is a special type of mathematics ☺

**Crypto Misconceptions

THIS IS WRONG:

- SHA-256 is a cipher and provides confidentiality.
  - Not it is a hash function and provides integrity of everything [hard to modify./cheat]



- "Bitcoins are encrypted": WRONG
  - ONLY if you encrypt your wallet, not everybody does.
  - Also can use SSL in P2P connections…
    - communications are encrypted if you use TOR

Block Chain

(and Mining - expanded much later)

Append-Only Logs

One well-known method to implement money
[pre-dates bitcoin according to George Danezis slides]:

A high-integrity, high-authenticity ”append only log”.

Sufficient to implement money in theory.

- Start by marking who has what money.
- Enter a log entry for each transfer.

Solutions differ in the method to get this ”append only log”

Bitcoin Mining

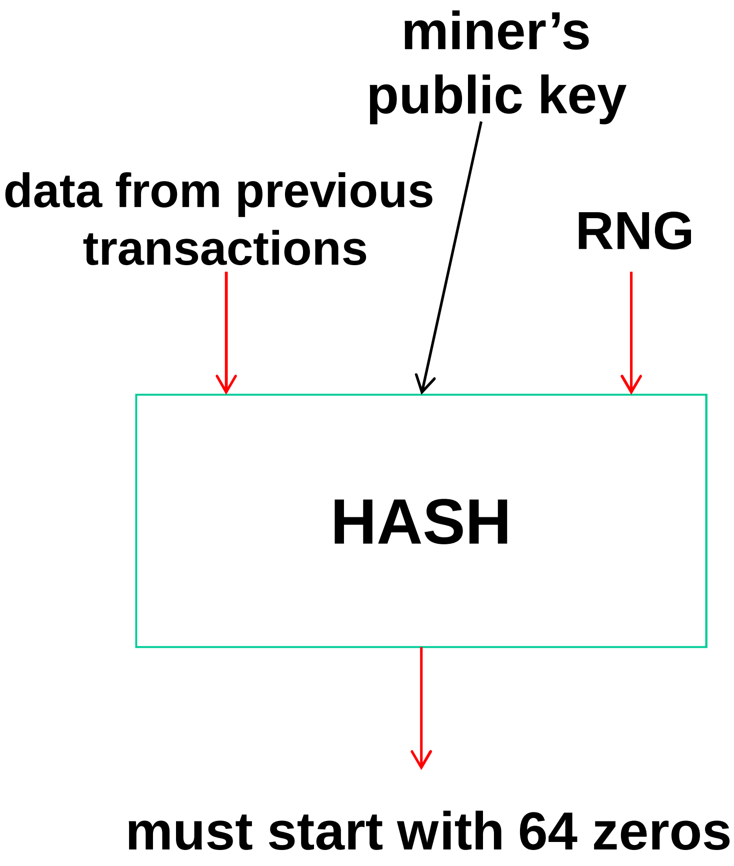
- Minting: creation of new currency.
- Confirmation+re-confirmation of older transactions

Random Oracle – like mechanism

Ownership:

- – "policed by majority of miners":
- – only the owner can transfer

[a part of] 25 BTC produced.



Block Chain

Def:

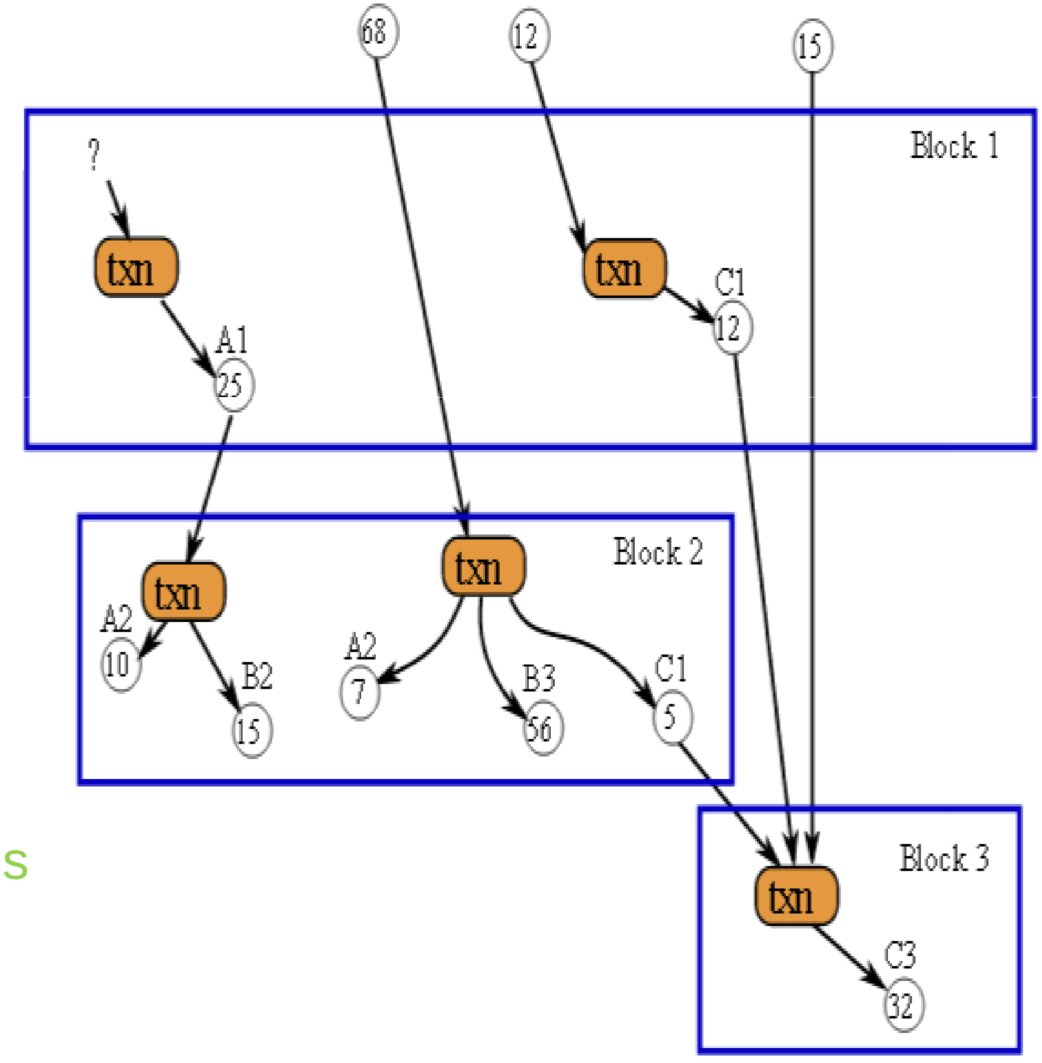
A transaction database
shared by everyone.

Also a ledger.

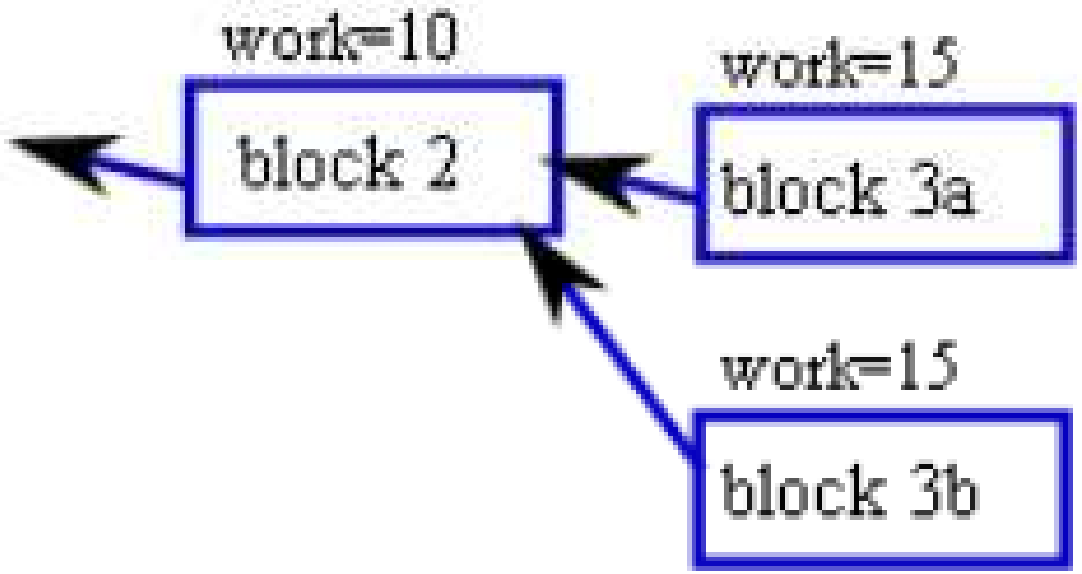
Every transaction
since ever is public.

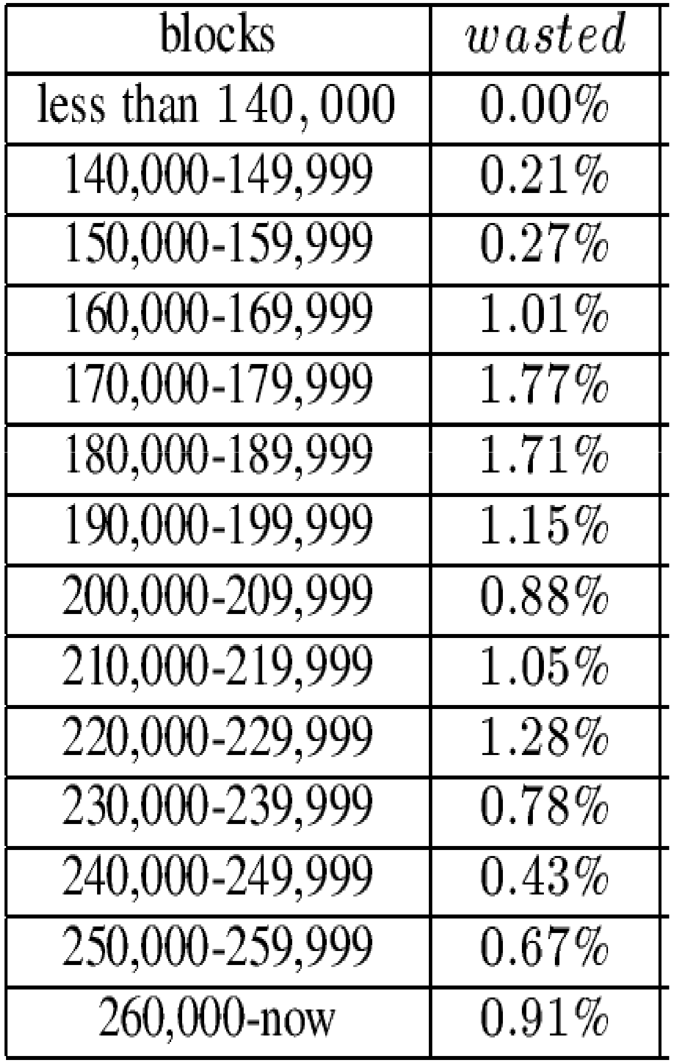
Each bitcoin “piece” is
a union of things uniquely traced
to their origin in time

(cf. same as for several banknotes
due to SN)



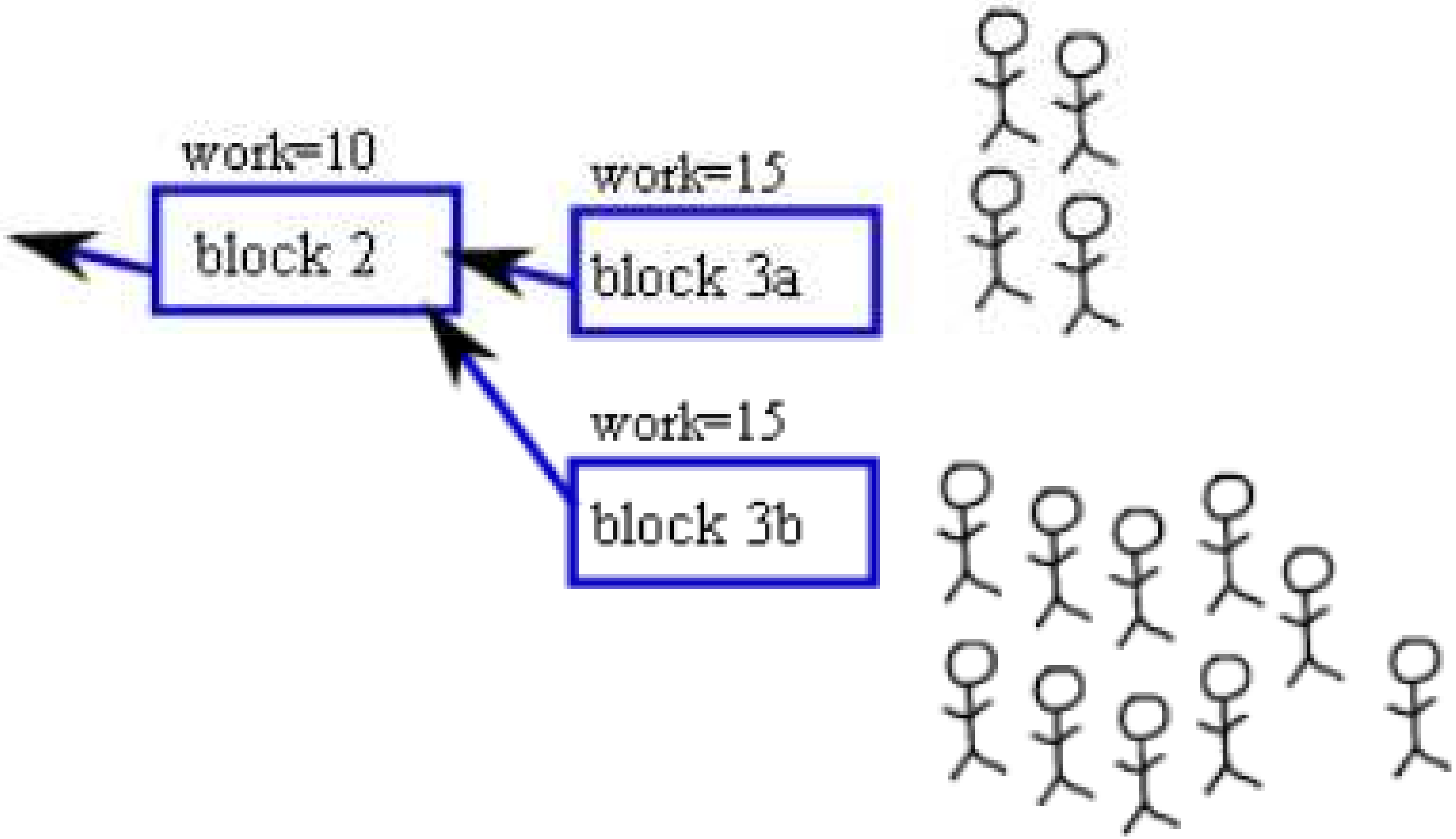
Fork – Hard To Avoid, 1% of the time





blocks	*wasted*
less than 140, 000	0.00%
140,000-149,999	0.21%
150,000-159,999	0.27%
160,000-169,999	1.01%
170,000-179,999	1.77%
180,000-189,999	1.71%
190,000-199,999	1.15%
200,000-209,999	0.88%
210,000-219,999	1.05%
220,000-229,999	1.28%
230,000-239,999	0.78%
240,000-249,999	0.43%
250,000-259,999	0.67%
260,000-now	0.91%

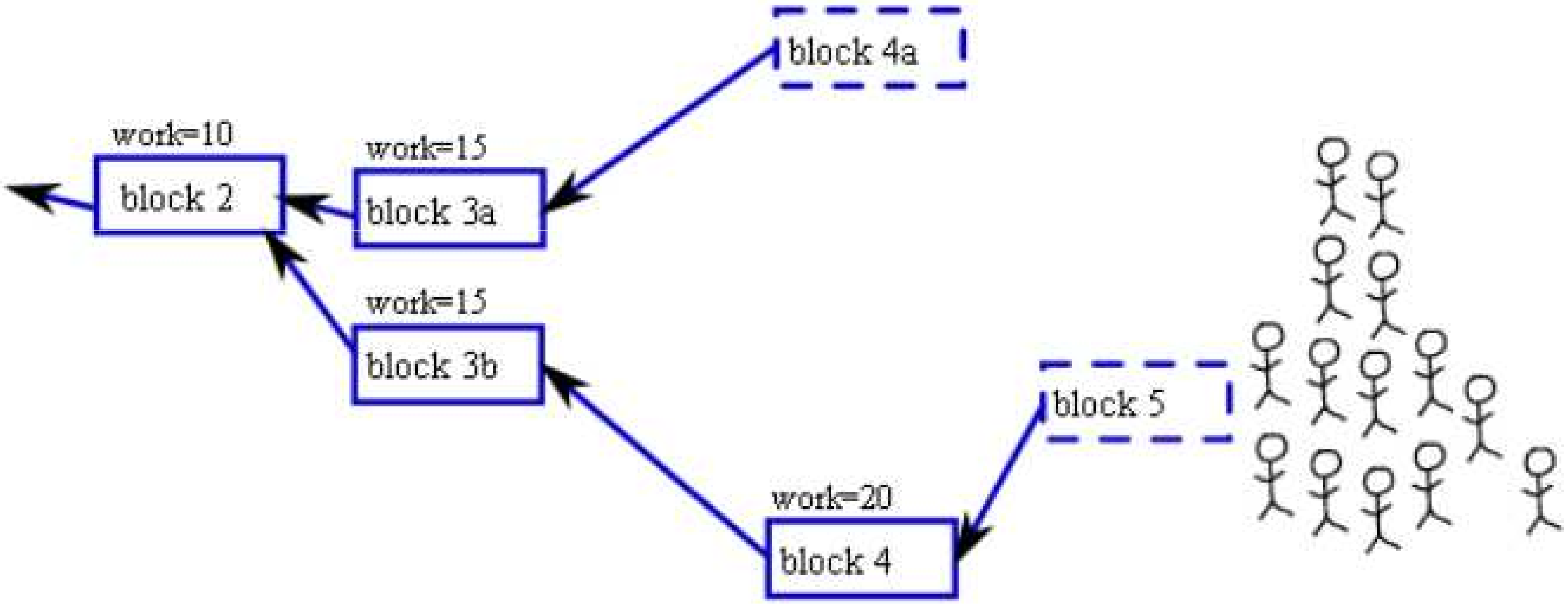
Fork – Miners Mine On Both Branches



Longest Chain Rule

[heavily criticised elsewhere]

“1 ASIC 1 vote”



Insight

If 2 solutions happens with proba 1/100

The chance that both will be extended before one of them reaches the miner of the other (making him stop) will be about

(1/100)^2

Etc..

Negligible chance to go on forever,
=> quite soon one branch is longer and wins.

Can Sb. Cancel His Transaction?

Yes if he produces a longer chain with another version of the history.

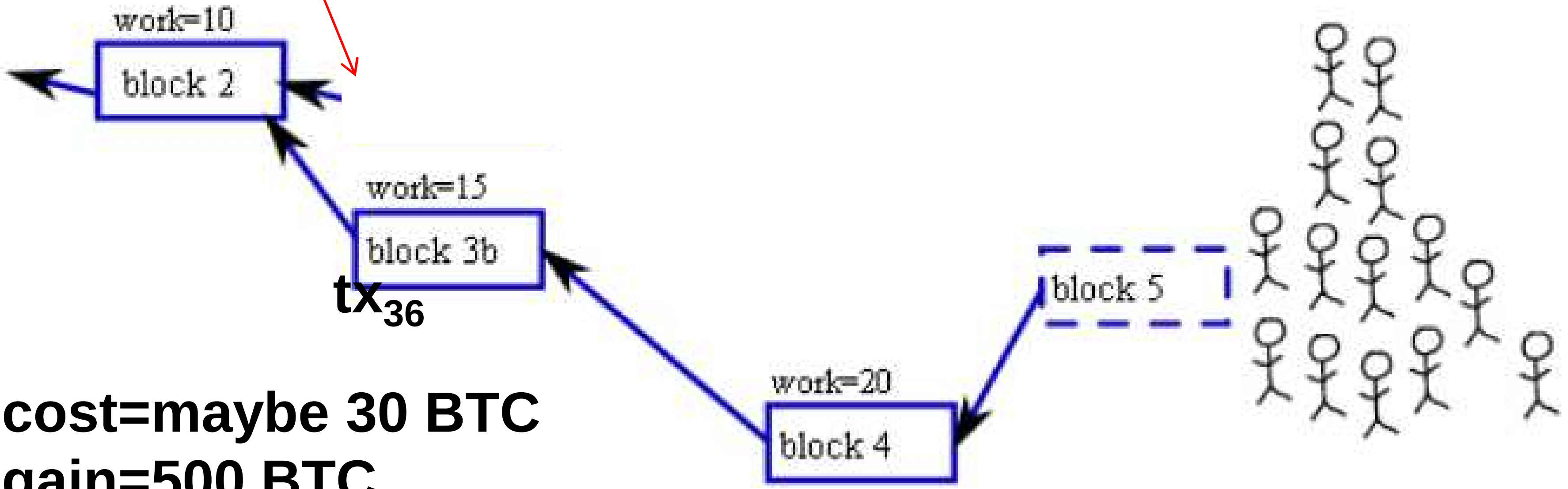
Very expensive, race against the whole network (the whole planet).

Can be easy or very difficult it depends!

Attack:

Extend This Branch To Cancel One Transaction tx_{36}

Goal: generate 4 blocks.



cost=maybe 30 BTC
gain=500 BTC
EASY and PROFITABLE!
The only difficulty is the timing!!!!

This Attack IS FEASIBLE!

Nicolas Courtois:

On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies http://arxiv.org/abs/1405.0534

Easy Or Difficult?

Difficult if:

- All mining devices are privately hold by independent people.

Easy if:

- Many mining devices are rented with a market which allows one instantly to buy a lot of hashing power by paying a small premium over the market price.

WORSE THAN THAT:

- A large mining pool can re-sell ALL the hash power to the attacker,

=> this CANNOT BE DETECTED by miners,
due to a technicality which we will discuss later
(mining with H0, not knowing on which branch/block they mine)

Is it a 51% Attack?

51 % attacks:

brain washing, vague and excessively general, highly misleading.

- computing power can be temporarily displaced.
- it is NOT a number between 0 and 100%, two different hash powers at different moments.

The Question of Dominance

This attack will NOT work if Bitcoin is dominant and uses more hash power than all other crypto currencies combined.

In contrast ALL SMALLER currencies which use a widely used hash function are EXTREMELY EASY to attack, and money can be stolen.

The Question of “The Longest Chain Rule”

The longest chain rule was designed to allow for EXTREMELY BAD NETWORK PROPAGATION (think of North Korea, Syria, yes bitcoin can function in such environments).

However with normal (fast) networks it is EASY just not to accept double spends after say 1 minute, and after one version of transaction is already propagated to a majority of network nodes.

⇒ Easy decision for miners. A majority needs to agree.

⇒ The longest chain rule is NOT good, needs reform.

Longest Chain Rule is PROBLEMATIC!

See:

Nicolas Courtois:

On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies http://arxiv.org/abs/1405.0534

No reason why the SAME rule would govern:

- Which block is paid (10 minutes)
- Which transactions are accepted (every second)

Violates the principles of

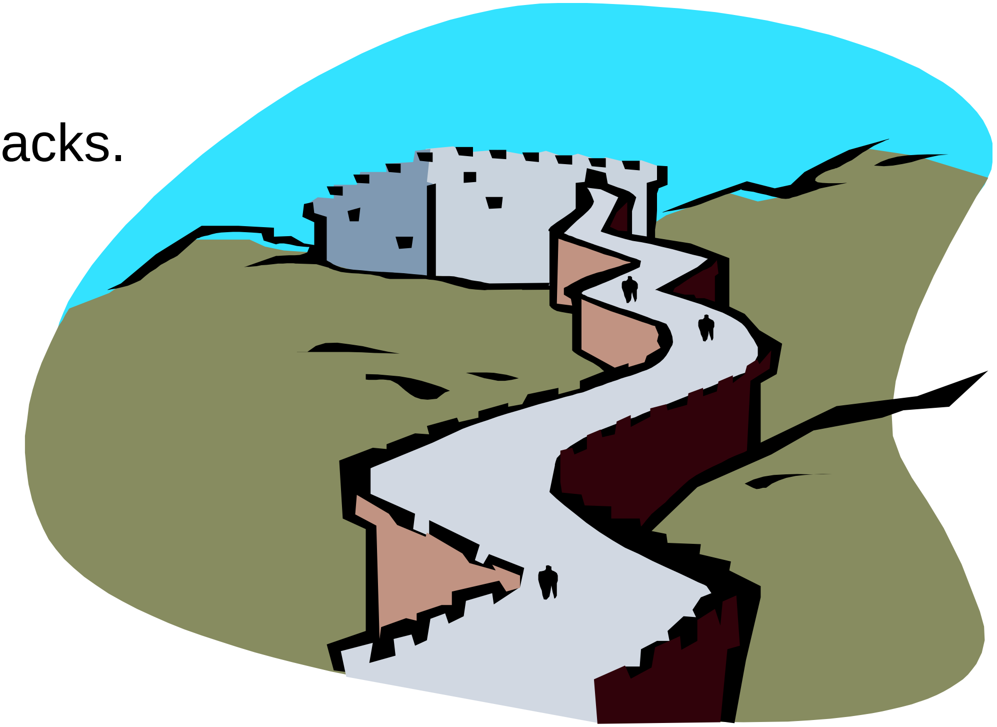
- Least Common Mechanism [Saltzer and Schroeder 1975]
- Poor Network Neutrality – miners have excessive discretionary powers…

=> Unnecessary instability and slow transactions…

Hash Power => Security???

Sams writes: "The amount of capital collectively burned hashing fixes the capital outlay required of an attacker […] to have a meaningful chance of orchestrating a successful double-spend attack […] The mitigation of this risk is valuable, [...]"

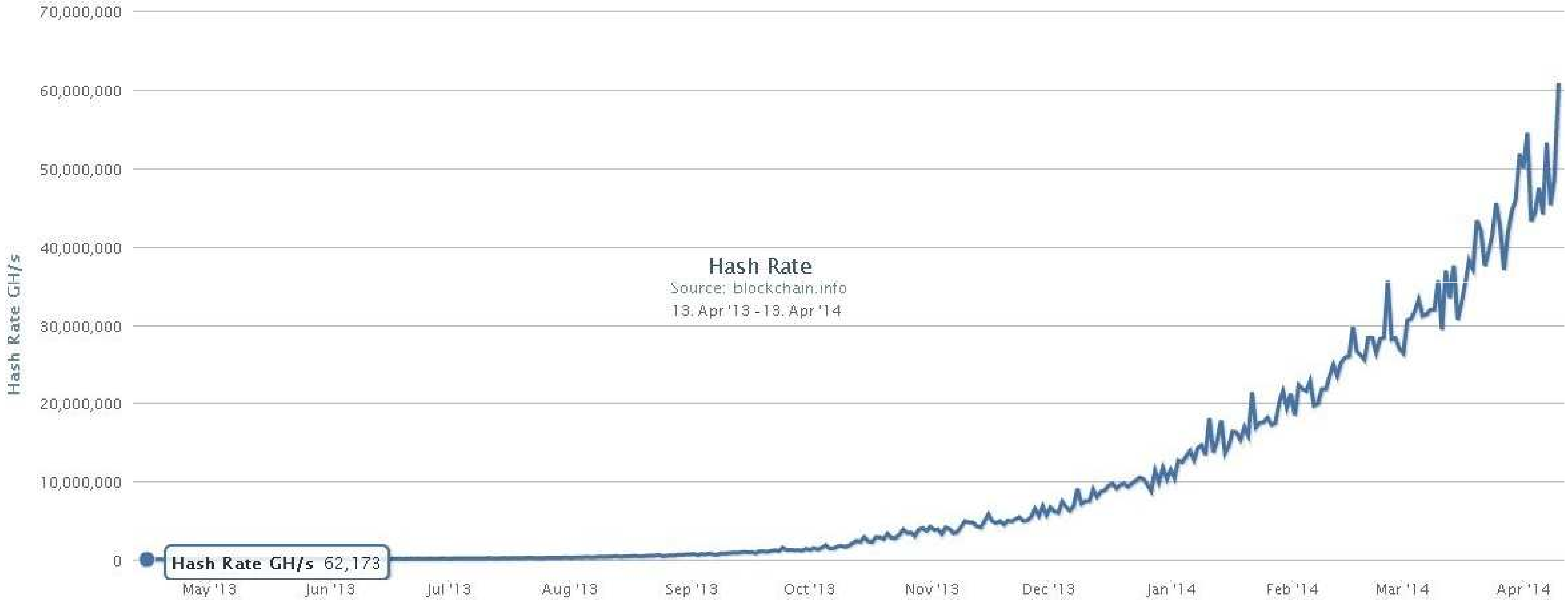
Wow! We have built a “Great Wall”.
It protects our money against attacks.



NO THIS IS MITAKEN

Crazy Hash Power Increase

Nearly doubled every month… 1000x in 1 year.



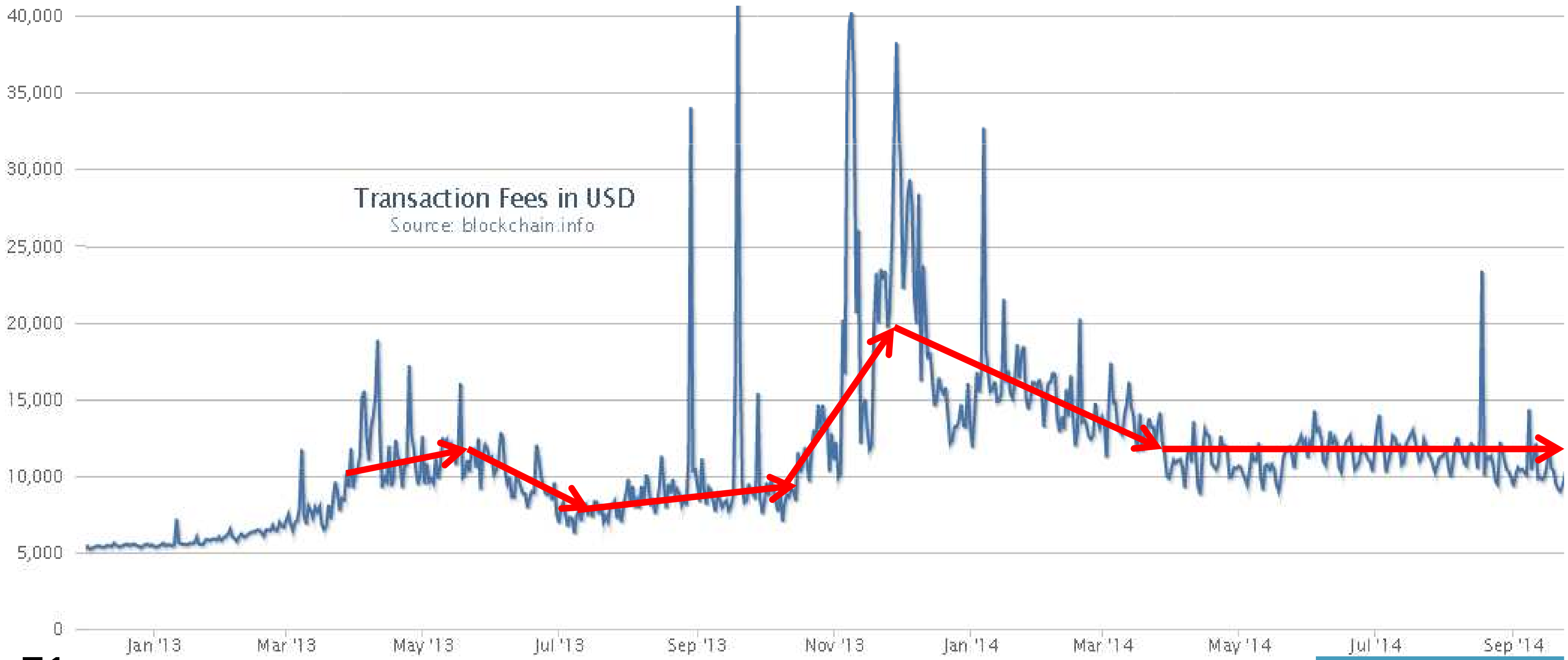
Thm:

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = 2$$

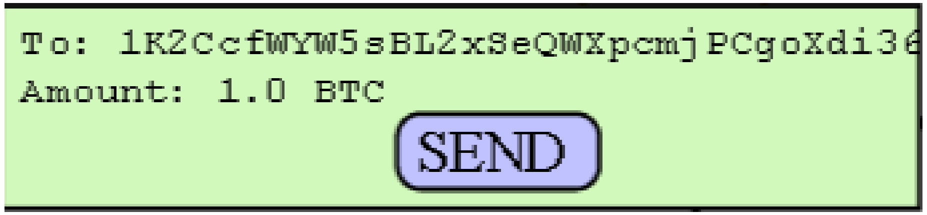
the total income is only **twice the income for the first month.**

In Contrast - Fees

Anybody willing to pay to use bitcoin?



Bitcoin Address



To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36

Amount: 1.0 BTC

Ledger-Based Currency

A “Bitcoin Address” = a sort of equivalent of a bank account.

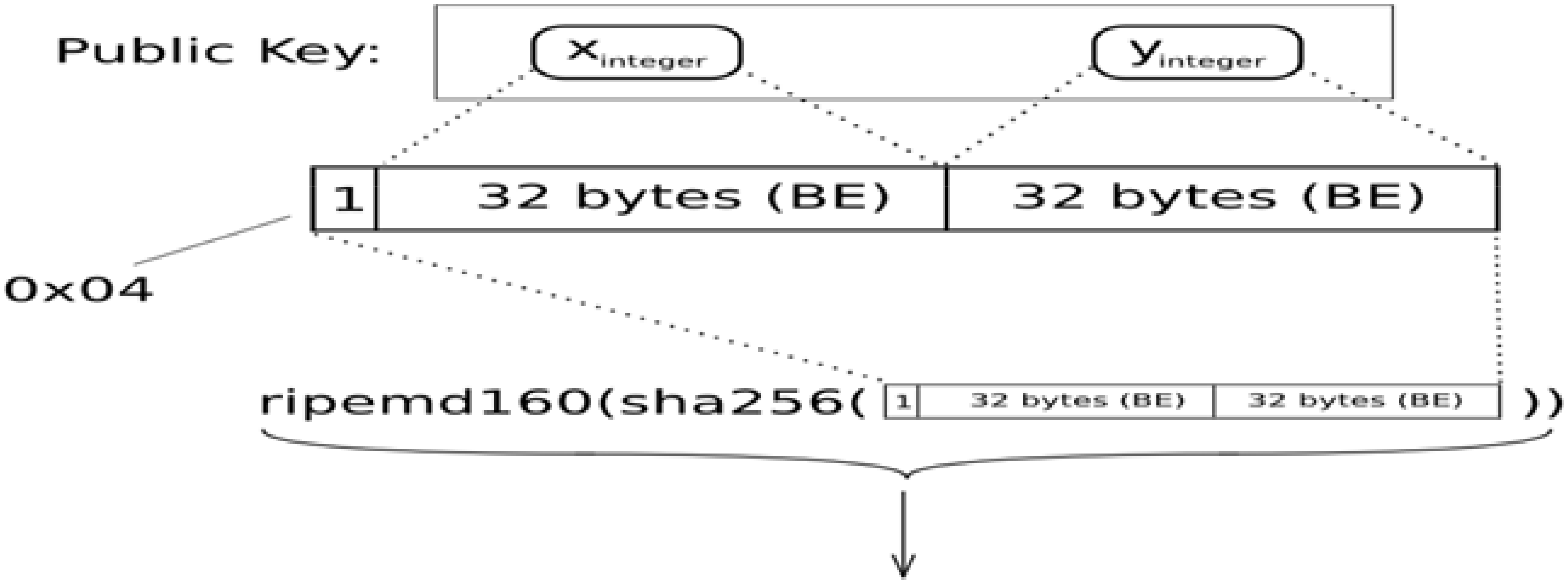
Three formats.

- First format like full Pkey 2*32 byte points, redundant!
  "scriptPubKey":"04a39b9e4fbd213ef24bb9be69de4a118dd0644082e47c01fd9159d38637b83fbcdc115a5d6e970586a012d1cfe3e3a8b1a3d04e763bdc5a071c0e827c0bd834a5 OP_CHECKSIG“
- Hash it on 160 bits, conceals the PK key! (NSA: attacks possible!).
  - e.g. 0568015a9facccfd09d70d409b6fc1a5546cecc6
- Recode with checksum on 1+20+4 bytes checksum, 160+32 bits,
  - Base58: 1VayNert3x1KzbpzMGt2qdqrAThiRovi8 27-34 chars

PK itself remains confidential until some part is spent.

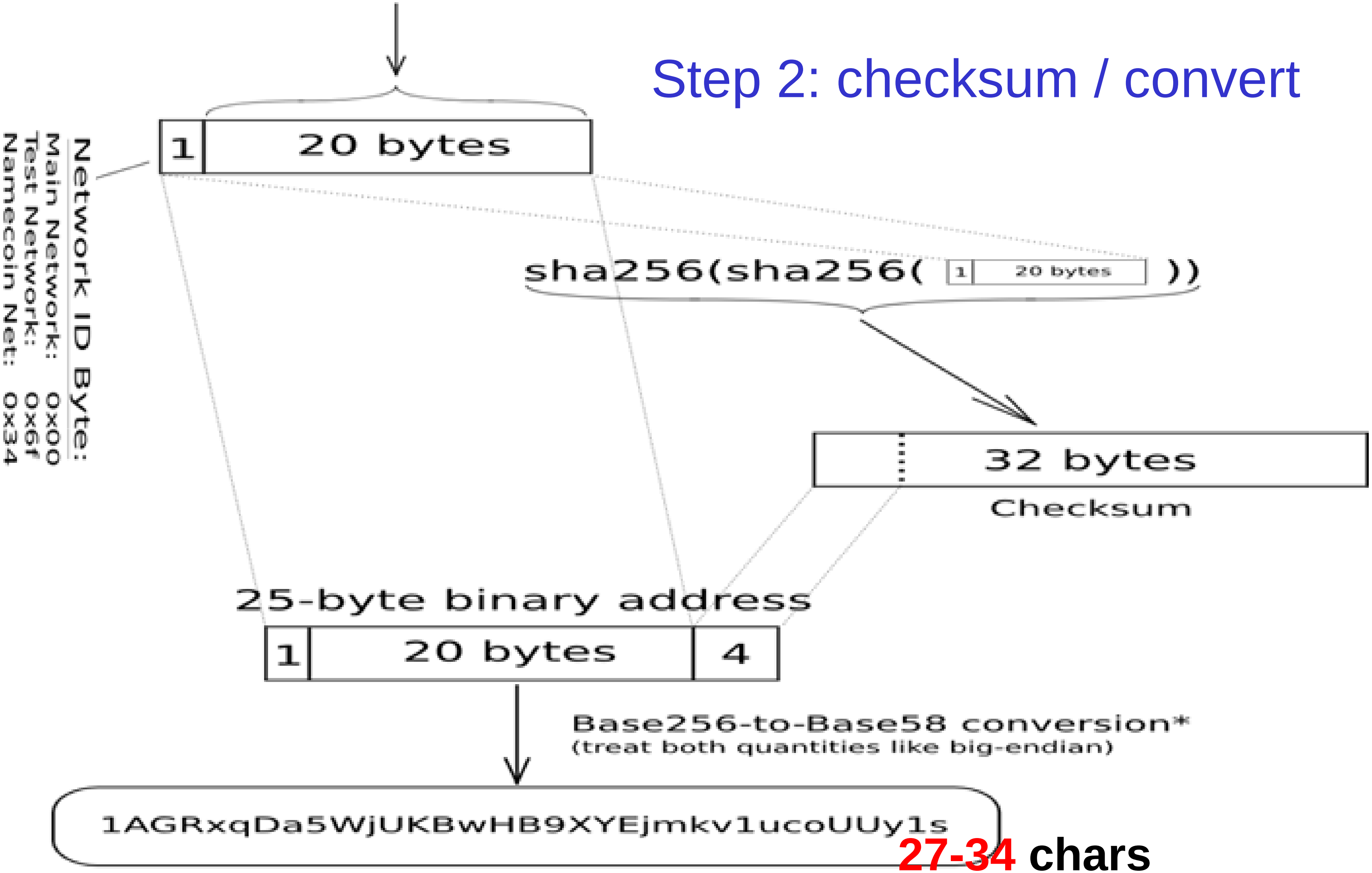
SK = private key is always kept private, allows transfer of funds.

Step 1: Hash



40 chars (nibbles)

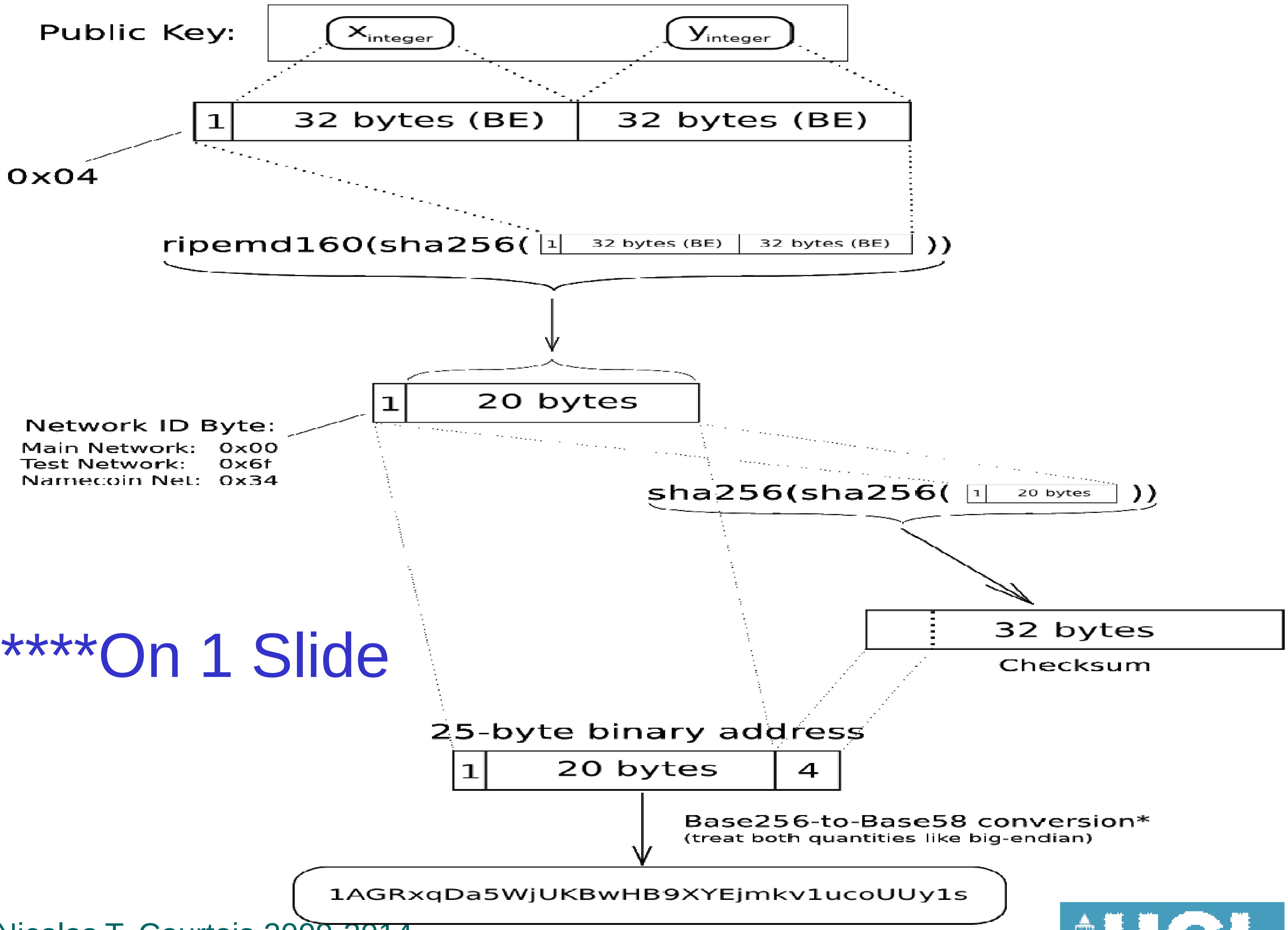
Step 2: checksum / convert


Network ID Byte:
Main Network: 0x00
Test Network: 0x6f
Namecoin Net: 0x34
1
20 bytes
sha256(sha256(1 20 bytes))
32 bytes
Checksum
25-byte binary address
1
20 bytes
4
Base256-to-Base58 conversion*
(treat both quantities like big-endian)
1AGRxqDa5WjUKBwHB9XYEjmkv1ucoUUy1s

27-34 chars

Base_58 **O0I1**

Elliptic-Curve Public Key to BTC Address conversion



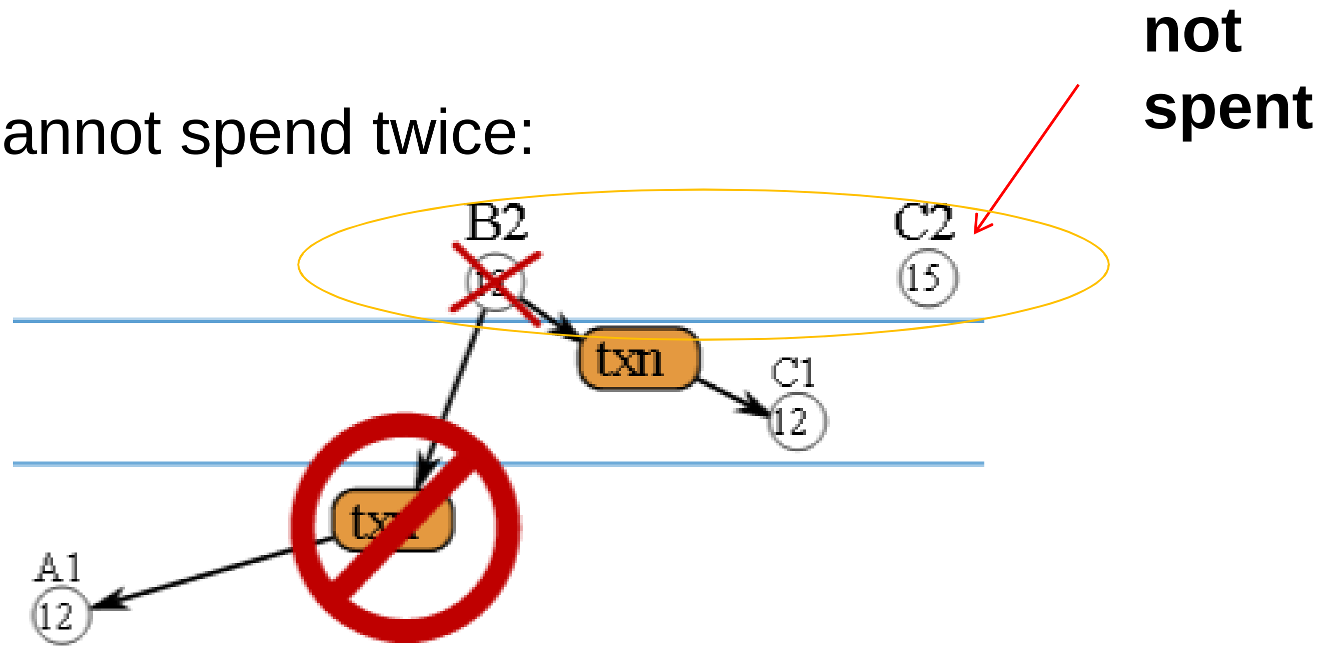
*****On 1 Slide

Bitcoin Ownership

Amounts of money are attributed to public keys.

Owner of a certain “Attribution to PK” can at any moment transfer it to some other PK (== another address).

Destructive, cannot spend twice:



Multi-Signature Addresses

Special Type of Addresses

Bitcoin can require simultaneously several private keys, in order to transfer the money.

The keys can be stored on different devices (highly secure).

They start with 3.

2 out of 3 are also already implemented in bitcoin [BIP16].

(1 device could be absent, money can still be used).

X out of 15 by the end of 2014…

Very cool, solves the problem of insecure devices…

Except if the attacker can break into many devices…

Multi-Sig Wallet Companies

- Clean business: they do NOT touch customer funds ever?

First was BitGo, August 2013

- 3 keys: BitGo, Custodian, Customer
- (more recently added HD Wallet support, what for?)
- login user/password==poor security! (however only 1 key…)
- business model: software as a service, also paid for storage?
- he has compared his business to VeriSign in early days…

Elliptic = UK bitcoin storage company

- AML: no problem at all, they keep all customer funds separated, no mixing ever.

Multi-Sig and BTC Storage Trends

Notes from CoinSummit conf 07/2014.

Good practices / trends:

- huge learning curve. Better done by specialists than every company…
- Move from storage to “custodianship”???
- Store MORE on blockchain (unlike current exchanges)! Except when need BTC very fast…

Bitcoin Circulation

To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36

Amount: 1.0 BTC

Bitcoin Myths (not true)

"Transactions are irreversible,"

- really???? The opposite can be argued:
  - – The Longest Chain Rule means probabilistic certitude,
    - HOWEVER in theory EVERY TRANSACTION CAN BE INVALIDATED, (at a large expense),

    ⇒possible even 100 years later

    ⇒if there is a longer chain!

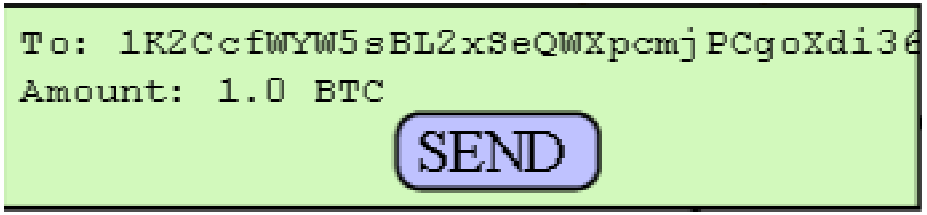
"No intermediary in transactions?"

- – Not true (unless one of the parties is a miner)

Bitcoin Transactions:

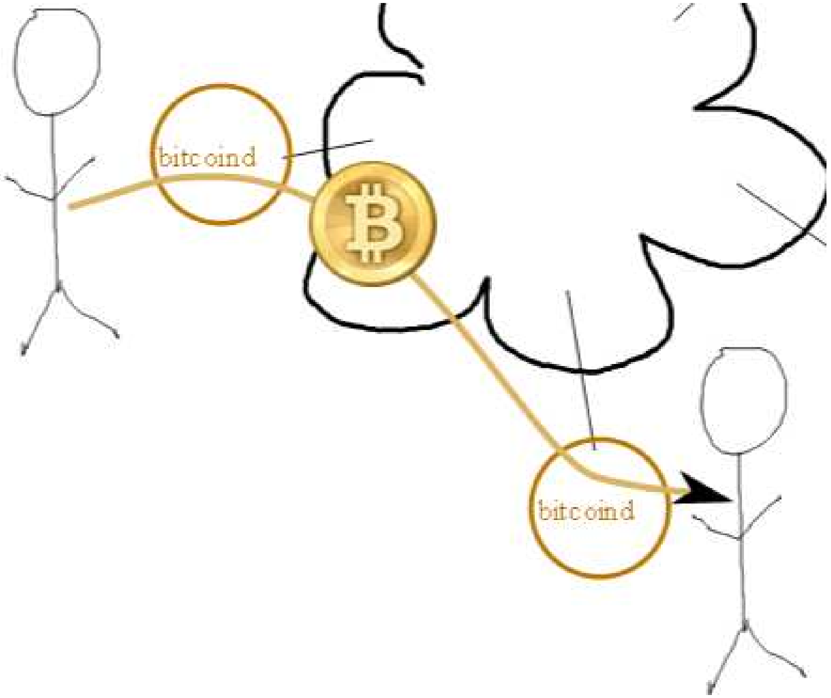
- between any two addresses [and any two network nodes],
  - at any time [no market closing hours].
  - validated within 10-60 minutes.
    - should wait longer for larger transactions, beware of “cheating miners”…
    - many websites accept instantly,
      - they trust your application not to double spend
      - and trust miners to reject the second spent based on later time, easy and plausible!

Transfer



To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36

Amount: 1.0 BTC

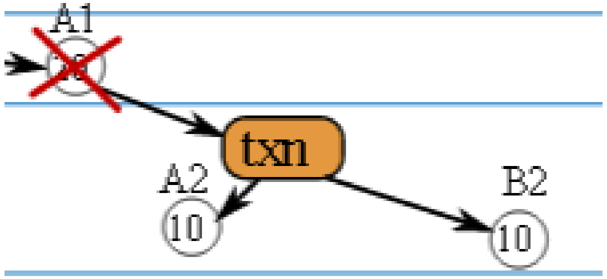


In / Out

Owner of a certain “Attribution to PK” can at any moment transfer it to some other PK addresses.

=> 0 inputs possible if minting transaction… new money.

=> Several outputs are a norm for bitcoin transactions.

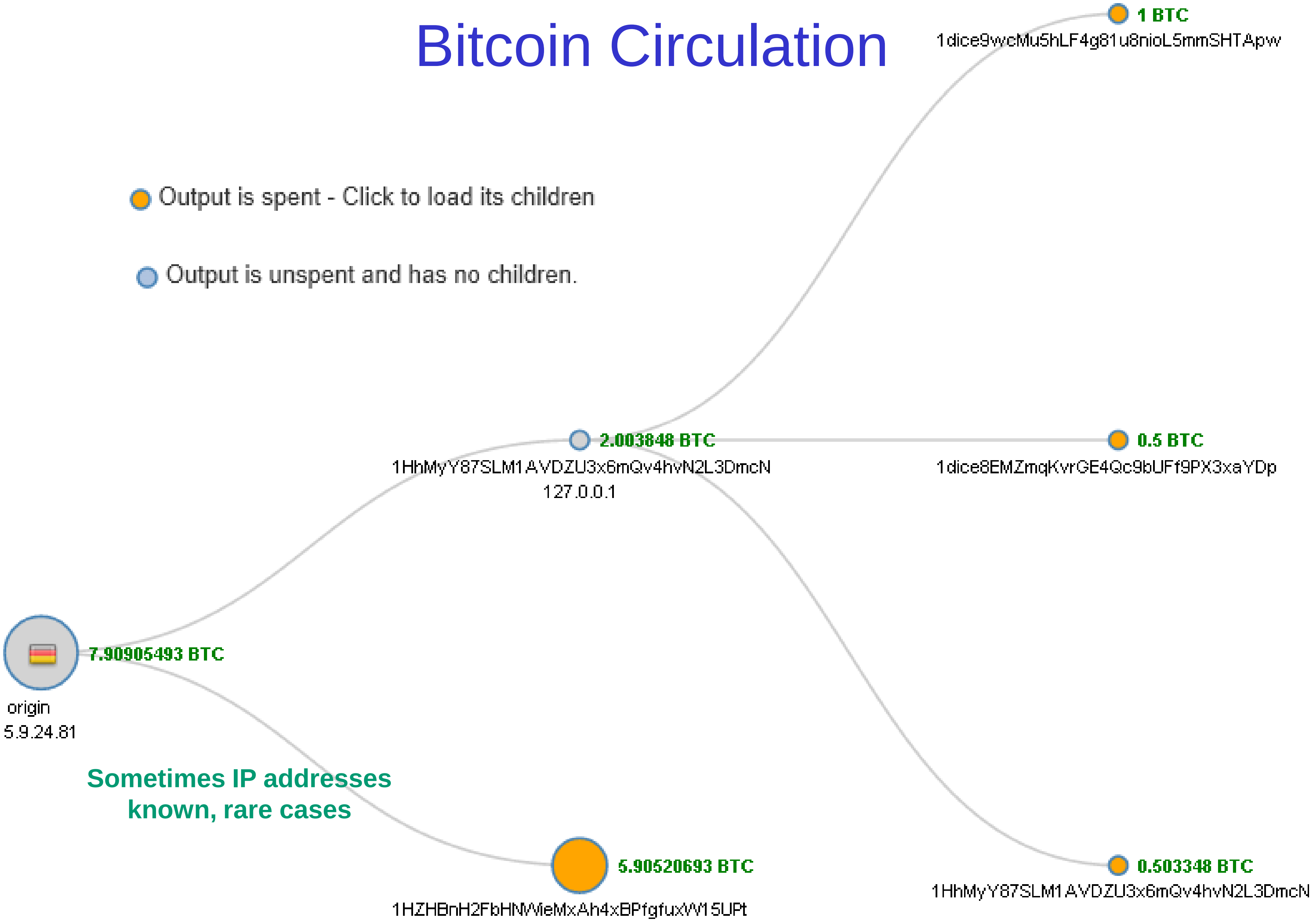


on this picture we ignore the fees

Bitcoin Transfer

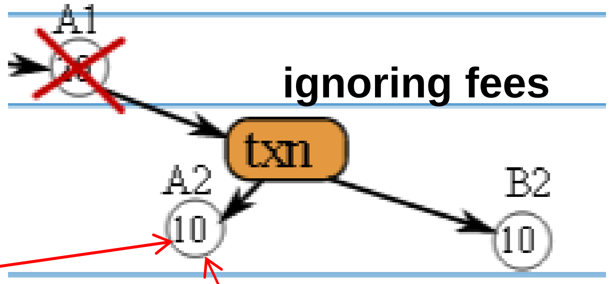
Owner of a certain “Attribution to PK” can at any moment transfer it to any other PK address.

Bitcoin Circulation


● Output is spent - Click to load its children
● Output is unspent and has no children.
1 BTC
1dice9wcMu5hLF4g81u8nioL5mmSHTApw
2.003848 BTC
1HhMyY87SLM1AVDZU3x6mQv4hvN2L3DmcN
127.0.0.1
0.5 BTC
1dice8EMZmqKvrGE4Qc9bUFf9PX3xaYDp
7.90905493 BTC
origin
5.9.24.81
5.90520693 BTC
1HZHBnH2FbHNWieMxAh4xBPfgfuxW15UPt
0.503348 BTC
1HhMyY87SLM1AVDZU3x6mQv4hvN2L3DmcN

Sometimes IP addresses known, rare cases

Attributions



ignoring fees

DEFINITION

"Attribution to PK" =

act of an owner of

a previous attribution (always destroyed)

which transfers a certain amount to the new PK = A2

(using a digital signature)

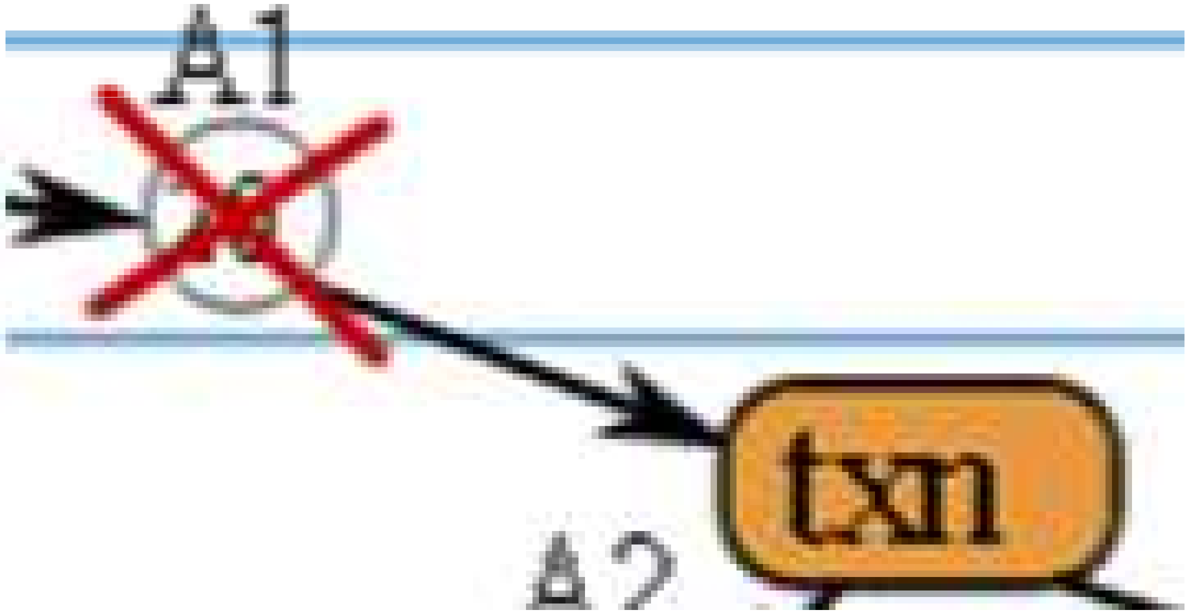
Caveat: Each attribution can be traced back to the initial mining event.

Fragmentation and Summation Rule

Each PK has a balance, say 20 BTC

current balance = sum(unspent attributions).

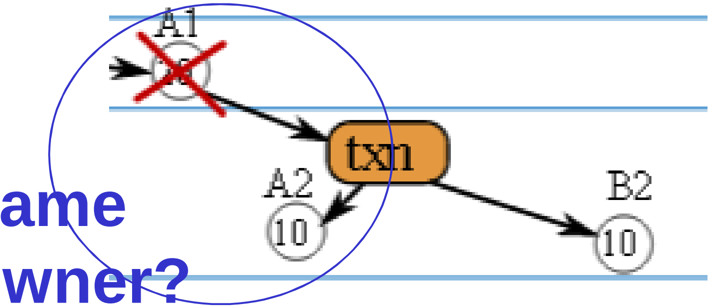
Attributions are ALWAYS destroyed when used,



From Single Attribution

Example

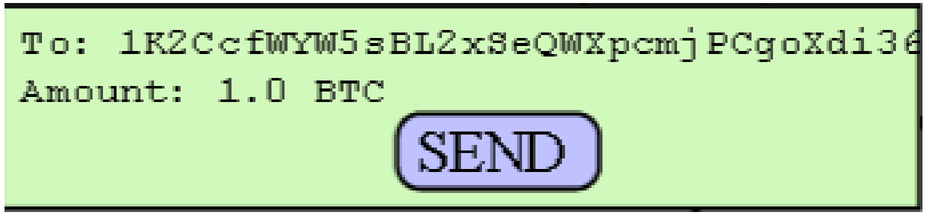
- Change: return some money to ourselves inside the same transaction
  - this implies most transactions have 2 or more outputs
  - most apps use the same address
  - could use another fresh address for better anonymity, but too lazy…



same owner?

no way to know for sure…

With Multiple Attributions



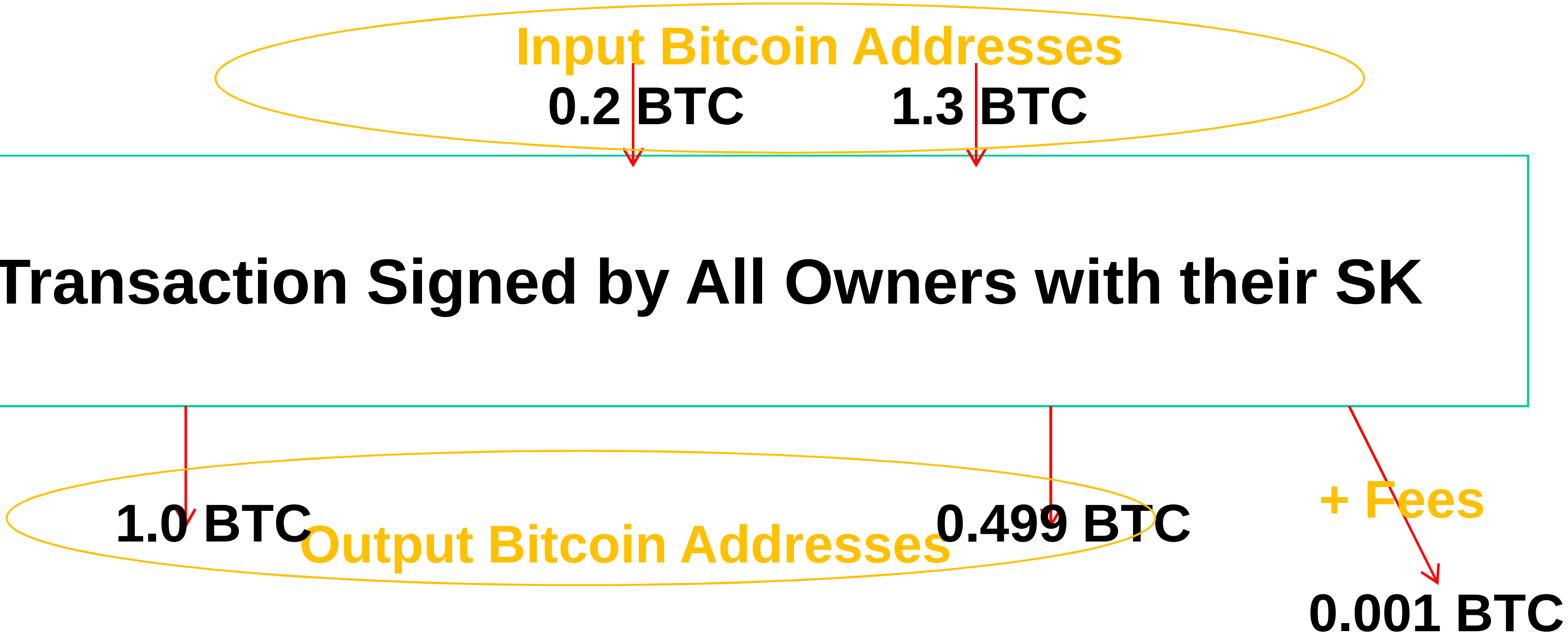
To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36

Amount: 1.0 BTC

typical case, even for a single user

Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



Input Bitcoin Addresses

0.2 BTC 1.3 BTC

Transaction Signed by All Owners with their SK

1.0 BTC Output Bitcoin Addresses 0.499 BTC

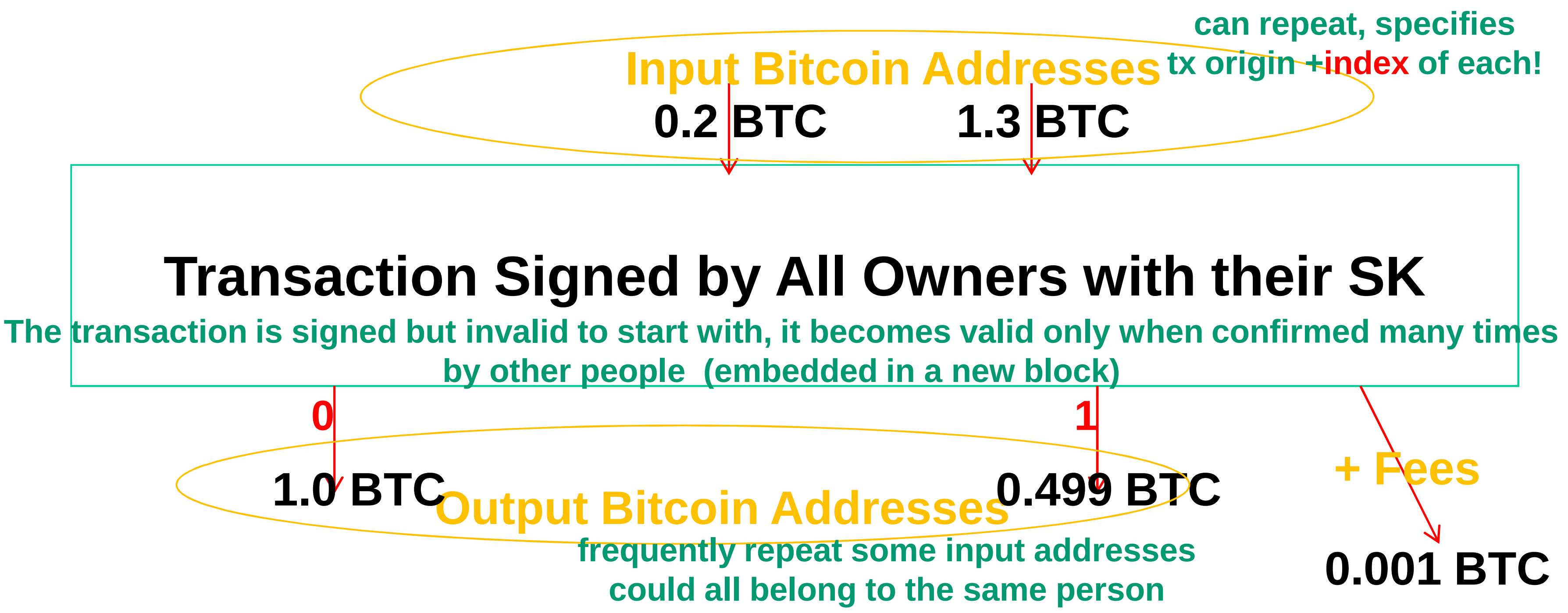
+ Fees

0.001 BTC

Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.

- helps for anonymity.
- destroys all current attributions,
- requires everybody's signature



can repeat, specifies tx origin +index of each!

Input Bitcoin Addresses

0.2 BTC 1.3 BTC

Transaction Signed by All Owners with their SK

The transaction is signed but invalid to start with, it becomes valid only when confirmed many times by other people (embedded in a new block)

0

1

1.0 BTC

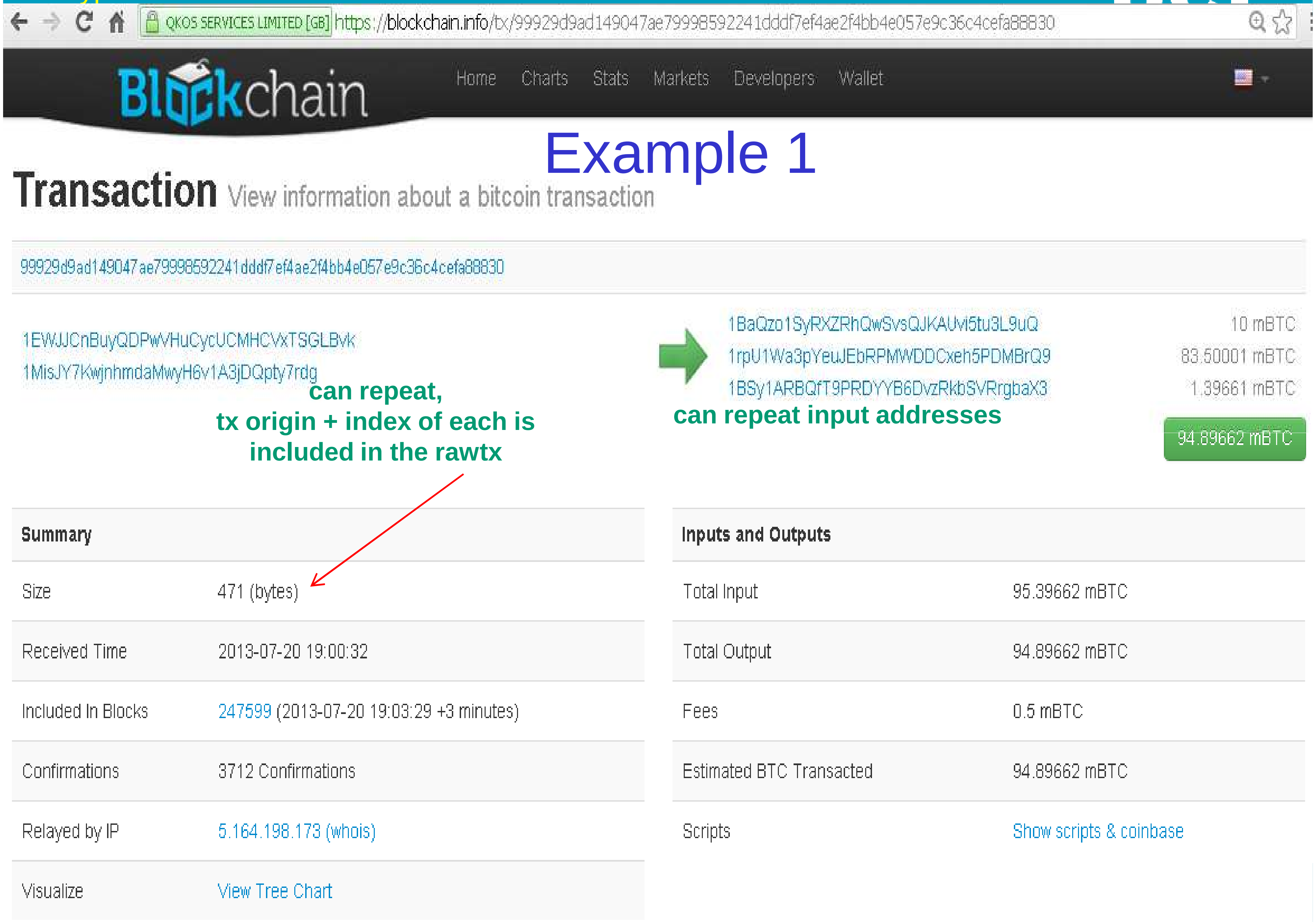
Output Bitcoin Addresses

0.499 BTC

+ Fees

0.001 BTC

frequently repeat some input addresses could all belong to the same person



QKOS SERVICES LIMITED [GB] https://blockchain.info/tx/99929d9ad149047ae79998592241dddf7ef4ae2f4bb4e057e9c36c4cefa88830

Example 1

Transaction View information about a bitcoin transaction

99929d9ad149047ae79998592241dddf7ef4ae2f4bb4e057e9c36c4cefa88830

1EWJJCnBuyQDPwVHuCycUCMHCVxTSGLBvk
1MisJY7KwjnhmdaMwyH6v1A3jDQpty7rdg

can repeat,
tx origin + index of each is included in the rawtx

1BaQzo1SyRXZRhQwSvsQJKAUvi5tu3L9uQ	10 mBTC
1rpU1Wa3pYeuJEbRPMWDDCxeh5PDMBrQ9	83.50001 mBTC
1BSy1ARBQfT9PRDYYB6DvzRkbSVRgbaX3	1.39661 mBTC

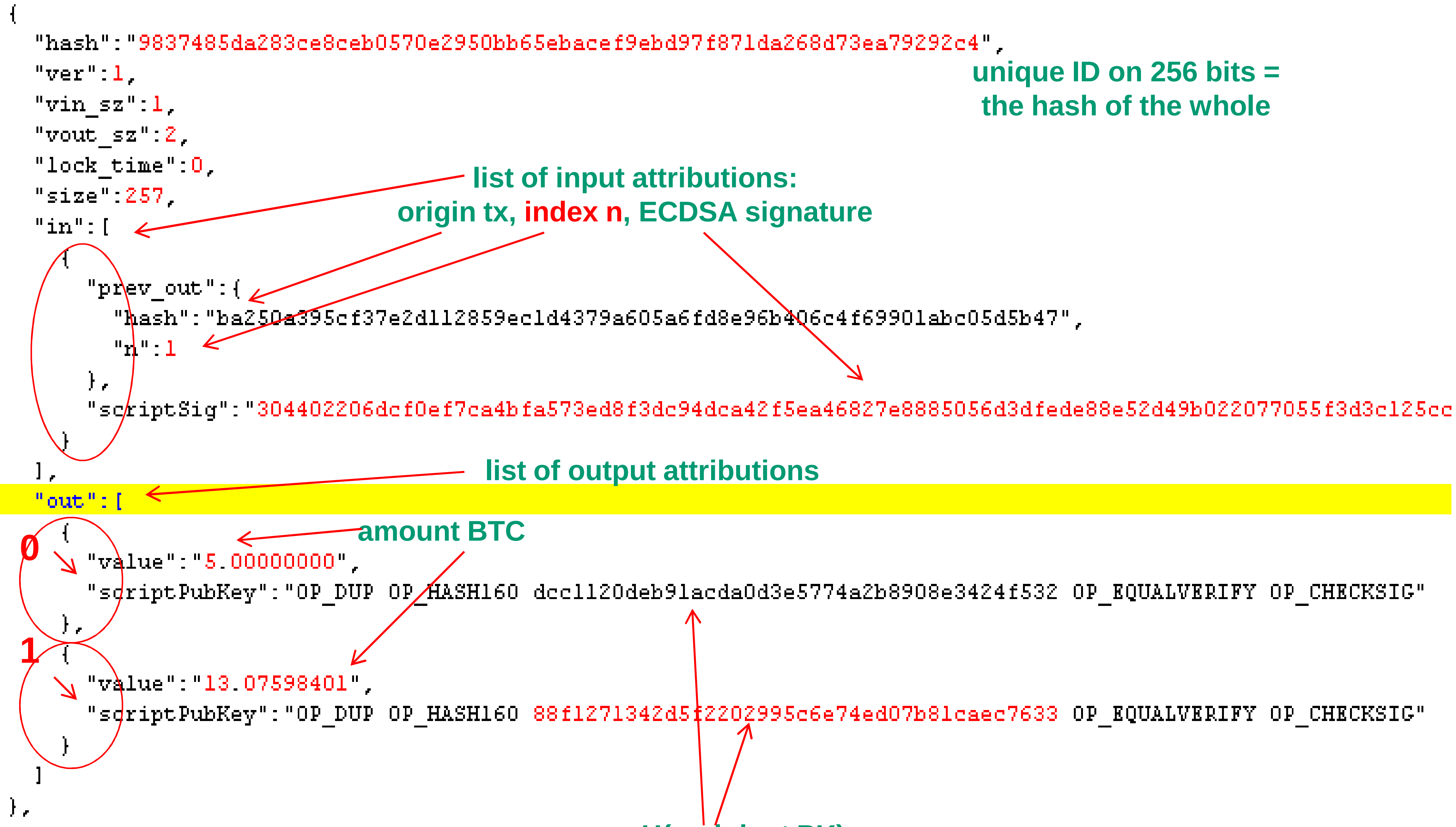
can repeat input addresses

94.89662 mBTC

Summary	
Size	471 (bytes)
Received Time	2013-07-20 19:00:32
Included In Blocks	247599 (2013-07-20 19:03:29 +3 minutes)
Confirmations	3712 Confirmations
Relayed by IP	5.164.198.173 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	95.39662 mBTC
Total Output	94.89662 mBTC
Fees	0.5 mBTC
Estimated BTC Transacted	94.89662 mBTC
Scripts	Show scripts & coinbase

Example 2 = Raw Transaction



```
{
  "hash":"9837485da283ce8ceb0570e2950bb65ebacef9ebd97f871da268d73ea79292c4",
  "ver":1,
  "vin_sz":1,
  "vout_sz":2,
  "lock_time":0,
  "size":257,
  "in":[
    {
      "prev_out":{
        "hash":"ba250a395cf37e2d112859ec1d4379a605a6fd8e96b406c4f69901abc05d5b47",
        "n":1
      },
      "scriptSig":"304402206dcf0ef7ca4bfa573ed8f3dc94dca42f5ea46827e8885056d3dfede88e52d49b022077055f3d3c125cc
    }
  ],
  "out":[
    {
      "value":"5.00000000",
      "scriptPubKey":"OP_DUP OP_HASH160 dcc1120deb91acda0d3e5774a2b8908e3424f532 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value":"13.07598401",
      "scriptPubKey":"OP_DUP OP_HASH160 88f1271342d5f2202995c6e74ed07b81caec7633 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
},
```

unique ID on 256 bits = the hash of the whole

list of input attributions:
origin tx, index n, ECDSA signature

list of output attributions

amount BTC

H(recipient PK)

Remarks:

About 30 million transactions ever made.

To know the balance of one account, we must “in theory” store ALL the transactions which send money for this address and then check ALL transactions made since then to see some of these are not already spent.

Full bitcoin network nodes stored all transactions ever made and checks their correctness (all the digital signatures).

About 15 Gbytes data, 24 hours full download.

In practice one could skip check for things confirmed by many miners… dangerous though. There is no absolute proof that miners have already checked them (maybe they forgot, a bug).

*Multiple signers:

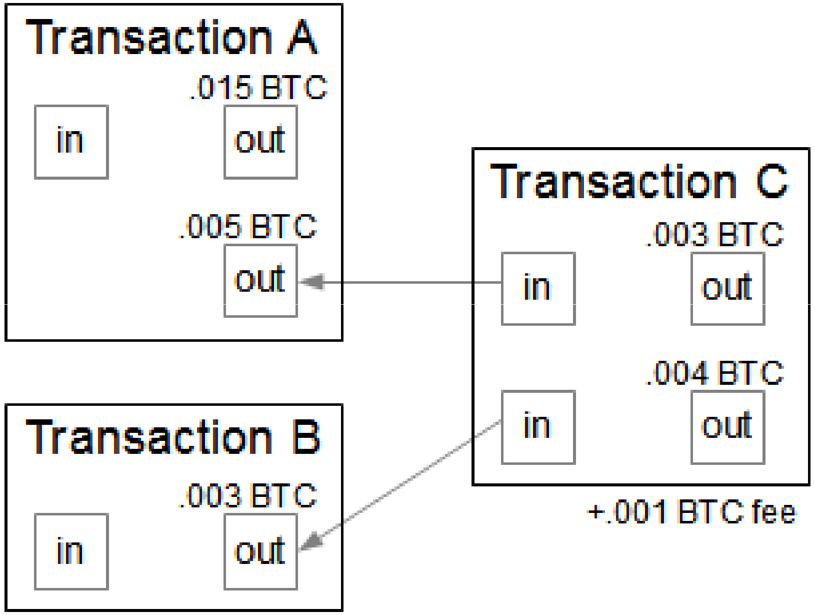
Issues:

- Who signs first?
  - In any order.
- What if one signs and other refuse?
  - Transaction is non-existent.
  - Cannot be used to sign something different.
- Do they KNOW what are they signing?
  - Yes, well, not sure

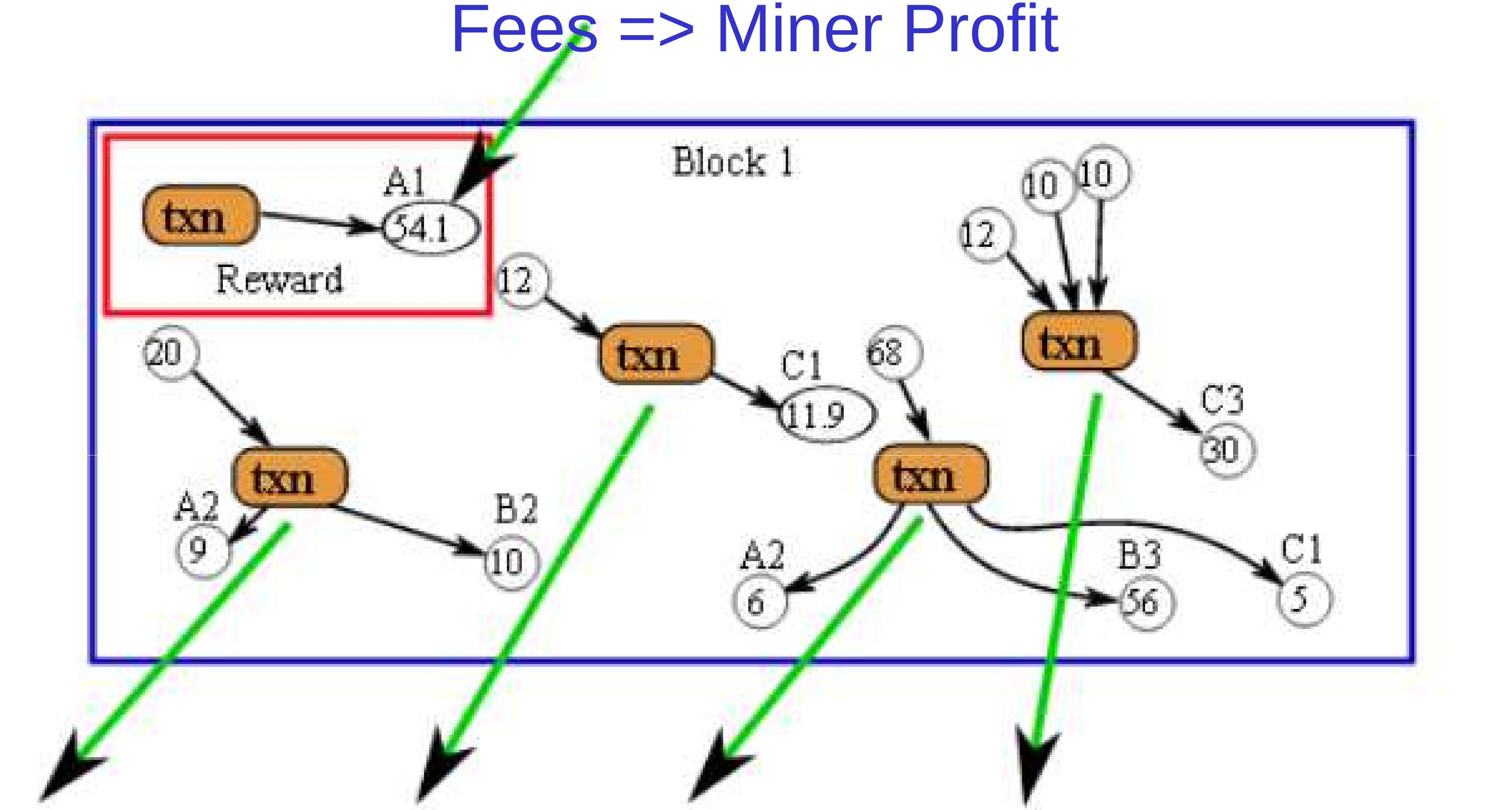
- What if some other inputs in this transaction are involved in illegal activity?

Transaction Chaining

2 attributions:



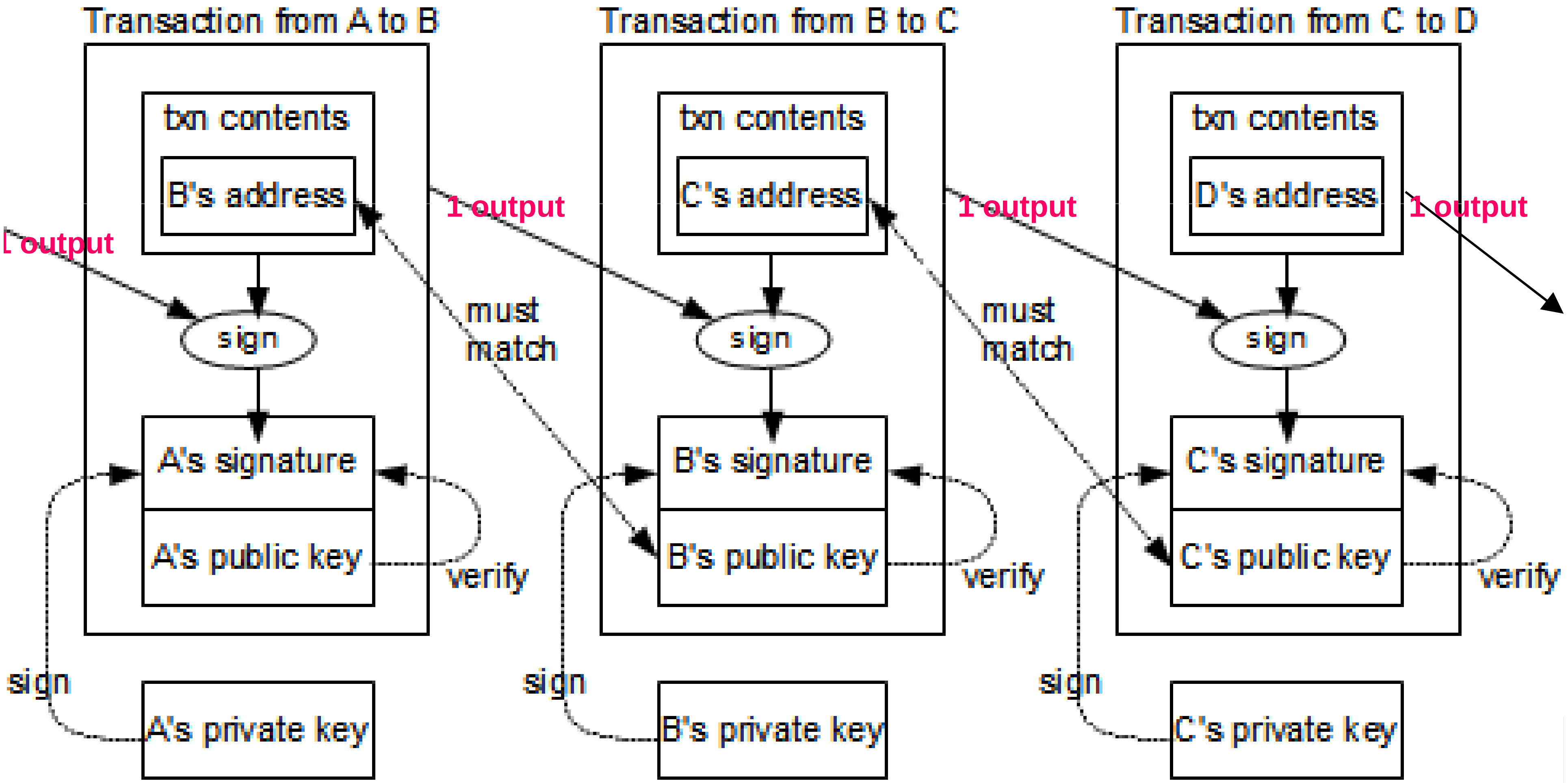
Fees => Miner Profit



1 + 0.1 + 1 + 2 = 4.1 (fees)
+ 50 (expansion)
= 54.1 (reward)

*Chaining and Checks

one branch of a tree:



What If FAQ

What If / Answer

- My private key or password is lost.
- I have an older backup for my wallet

What If / Answer

What If	Answer
My private key or password is lost.	All money is lost, NOBODY can recover it
I have an older backup for my wallet	Some money will be recovered, not all.

TED JUST REALIZED THAT HE ACCIDENTALLY FORMATTED THEWRONG HARD DISK, AND LOST HIS WALLET!
IT WAS A GOOD THING THAT HE BOUGHT THE GUN FOR BTC'S LAST WEEK!
C:>_
THE BITCOIN COMIC
BY Z1XWITCH
TOO BAD HE FORGOT BULLETS!

What If / Answer

- My private key or password is lost.
- I have an older backup for my wallet
- Password is easy guess
- RNG is faulty

- All money is lost, NOBODY can recover it
- Some money will be recovered, not all.

What If / Answer

My private key or password is lost.	All money is lost, NOBODY can recover it
I have an older backup for my wallet	Some money will be recovered, not all.
Password is easy guess RNG is faulty	My money will be stolen by an anonymous hacker ASAP.