Bitcoin,
Mining
and Stratum Protocol

Nicolas T. Courtois
Pinar Emirdag, Zhouyixing Wang
- **U**niversity **C**ollege **L**ondon, UK

Dr. Nicolas T. Courtois

1. cryptologist and codebreaker


IARIA
International Academy, Research, and Industry Association
BEST PAPER AWARD
Multiplicative Complexity and Solving Generalized Brent Equations With SAT Solvers
By
Nicolas Courtois, Daniel Hulme, Theodosis Mourouzis
Presented during COMPUTATION TOOLS 2012, The Third International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking, held in Nice, France - July 22-27, 2012
IARIA Board

UNIVERSITY CIPHER CHAMPION

March 2013

Cyber Security Challenge UK

2. payment and smart cards (e.g. bank cards, Oyster cards etc…)

Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

My Whole Life:

Tried to improve
the security baseline…

Crying Wolf!

Bitcoin Elliptic Curve,
51% Attack, OpenSSL...

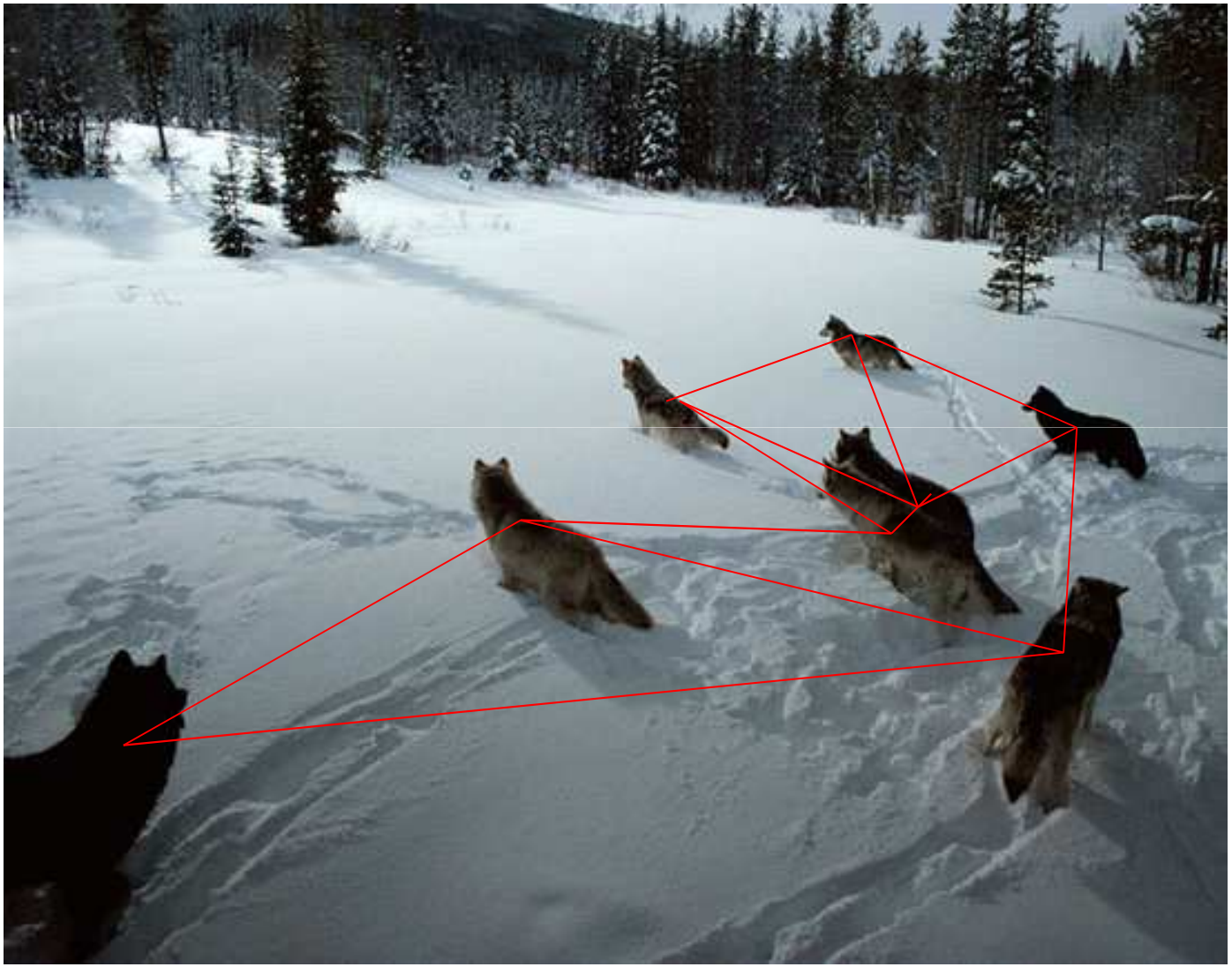
It did NOT help,

The Wolf was allowed to operate

We failed to protect our DATA

We failed to protect our MONEY

Solution = Decentralized P2P



Solution = BlockChain

- Until recently, we've needed central bodies – banks, stock markets, governments, police forces – to settle vital questions.
  - Who owns this money?

- 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]

The Telegraph
The coming digital anarchy

UCL Bitcoin Seminar

a crypto currency **research** seminar

in central London

public web page:

blog.bettercrypto.com

Today's slides, extended version (200 slides):

http://www.nicolascourtois.com/bitcoin/paycoin_mining_attacks_4.pdf

Our Works on Bitcoin

-cf. also blog.bettercrypto.com

-Nicolas Courtois, Marek Grajek, Rahul Naik: The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining, http://arxiv.org/abs/1310.7935

-Nicolas Courtois, Marek Grajek, Rahul Naik: Optimizing SHA256 in Bitcoin Mining, CSS 2014.

-Nicolas Courtois, Lear Bahack: On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency http://arxiv.org/abs/1402.1718

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

-Nicolas T. Courtois, Pinar Emirdag and Daniel A. Nagy: Could Bitcoin Transactions Be 100x Faster? In proceedings of SECRYPT 2014, 28-30 August 2014, Vienna, Austria.

-Poster: http://www.nicolascourtois.com/bitcoin/POSTER_100x_Secrypt2014_v1.0.pdf

-Nicolas T. Courtois, Pinar Emirdag and Filippo Valsorda: Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events, 16 Oct 2014, http://eprint.iacr.org/2014/848

-Nicolas T. Courtois, Pinar Emirdag and Zhouyixing Wang: On Detection of Bitcoin Mining Redirection Attacks, proc. of ICISSP 2015, Feb 2015.

Krugman

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

– Paul Krugman,
Nobel price in economics

Are They Crazy?

Anything can be “money”
if sufficiently many people accept it… (e.g. salt).

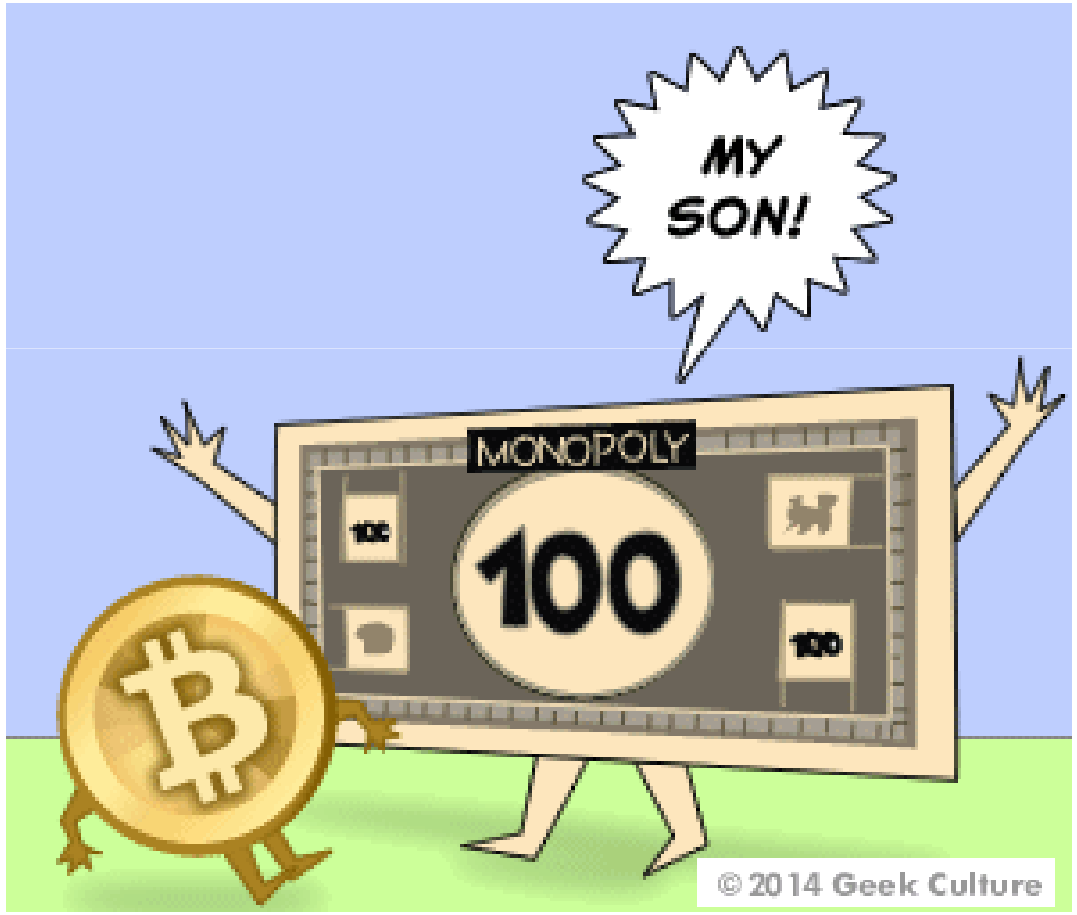
Question of:

- popularity
- trust

NO NEED TO TRUST ANYONE IN BITCOIN????

Play Money?

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

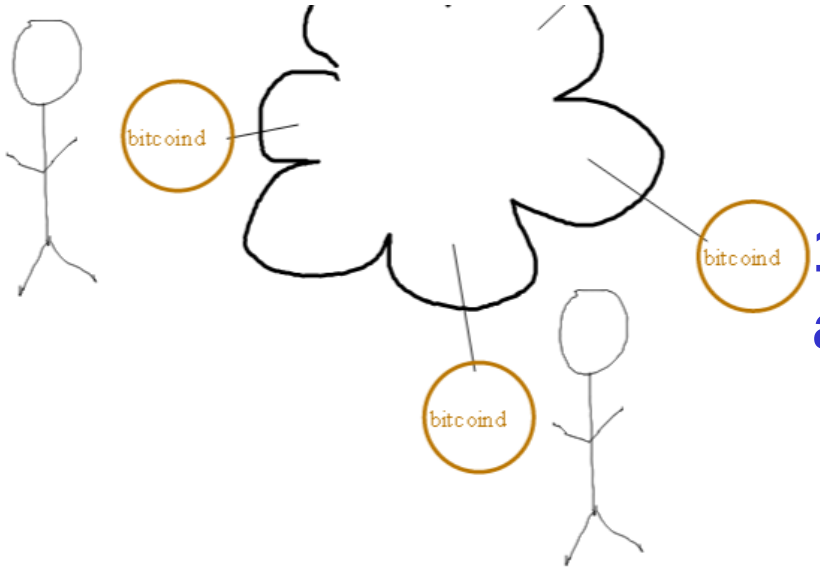


P2P Payment

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

Network

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

- homogenous nodes: they do the same job
  - everybody participates equally
  - everybody is mining

The Reality is VERY Different!

Tx LifeCycle

- Miner nodes
- Peer Nodes
- Wallet Nodes

burn

public ledger

tx

tx

*Panic – May 2014

- # active nodes << #miners
- 6K << 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

Bitcoin Wallets

- Wallet:
  - computer file which stores "the money".
  - Storing ECDSA private keys

Main Problem:

Bitcoins could be “spent twice”.

⇒Main problem when designing a digital currency system.

⇒Solution: all transactions are public.

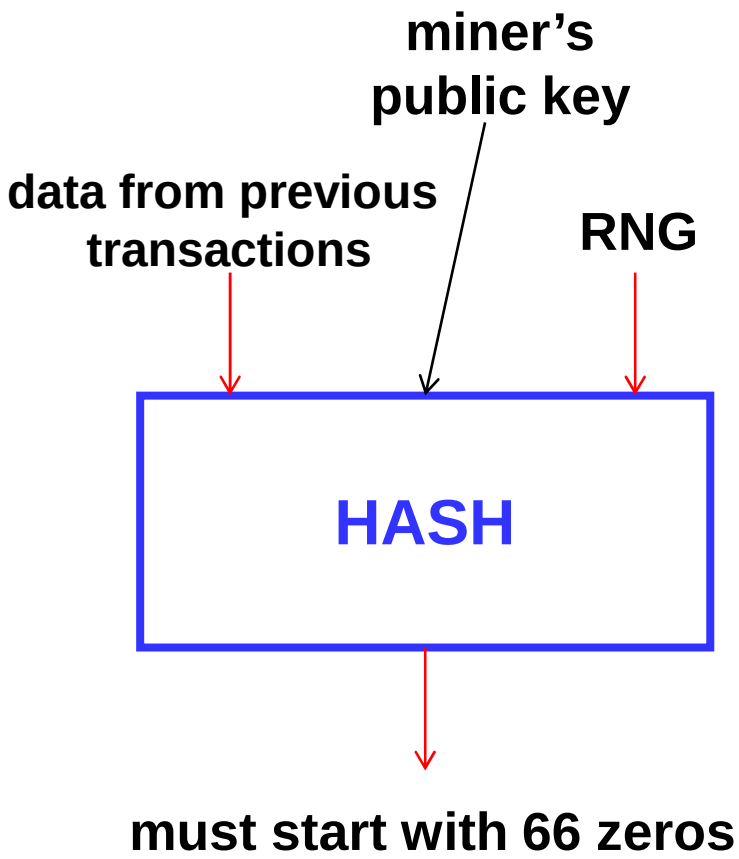
⇒Adding new transactions has a cost.

Block Chain

and Mining

Bitcoin Mining

- Creation of new currency.
- Confirmation+re-confirmation of older transactions

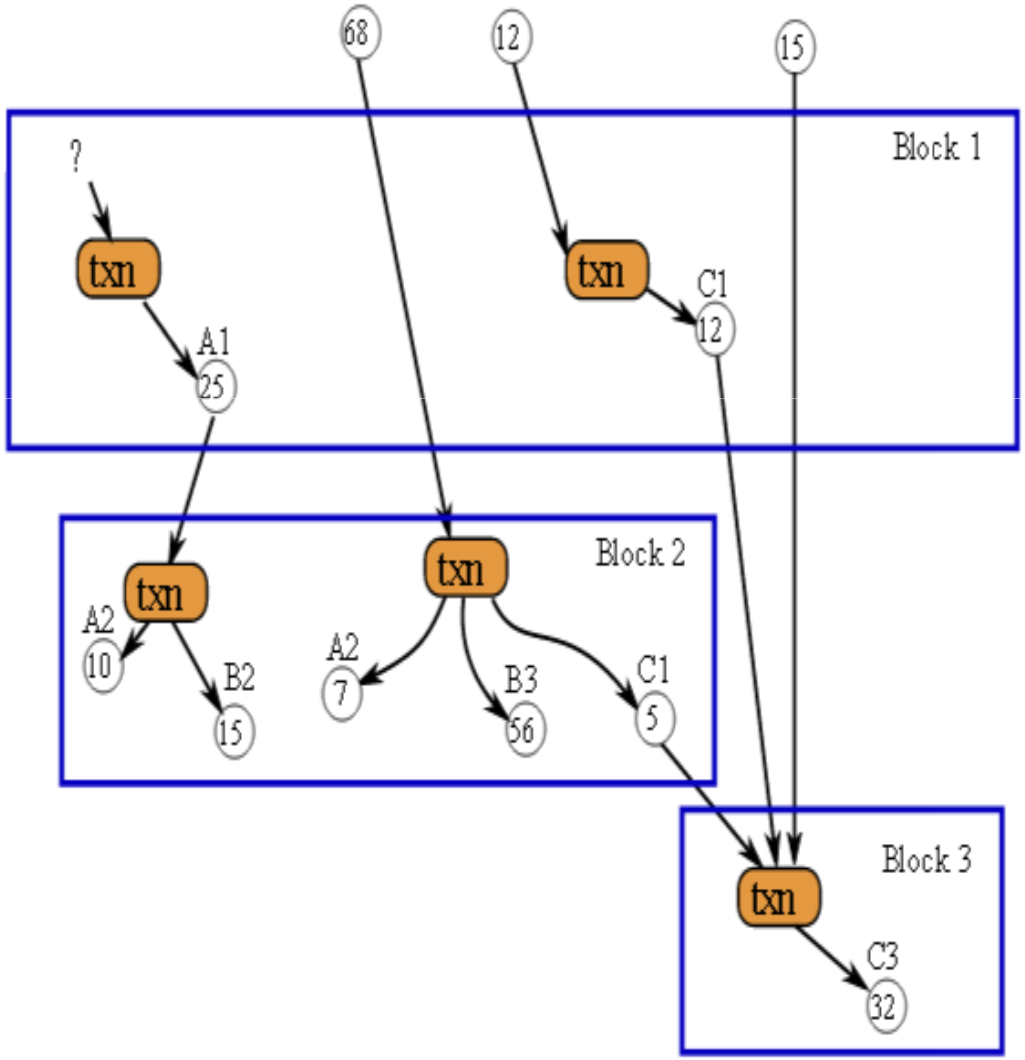


Block Chain

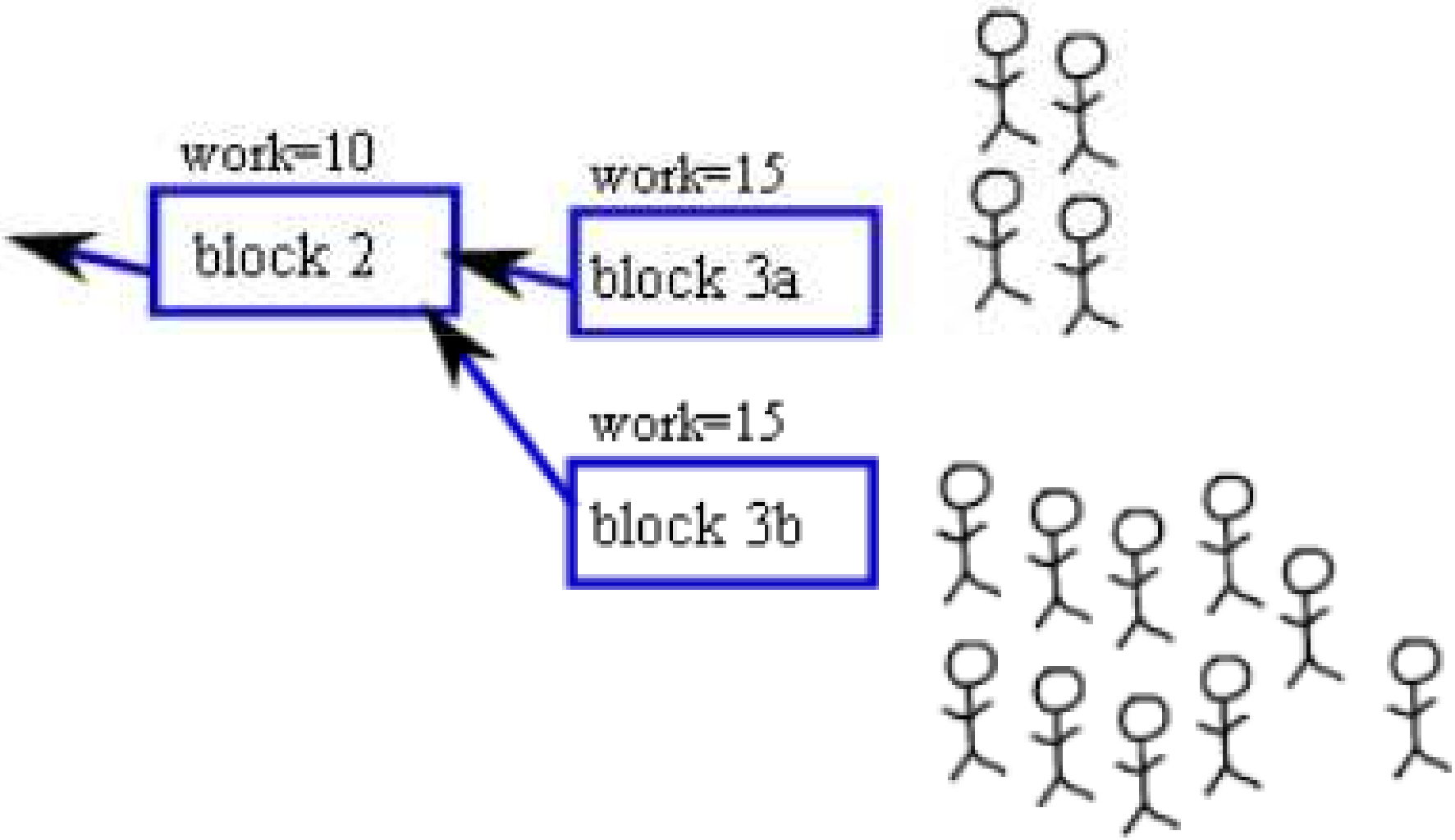
Def:

A transaction database shared by everyone.

Every transaction since ever is public.



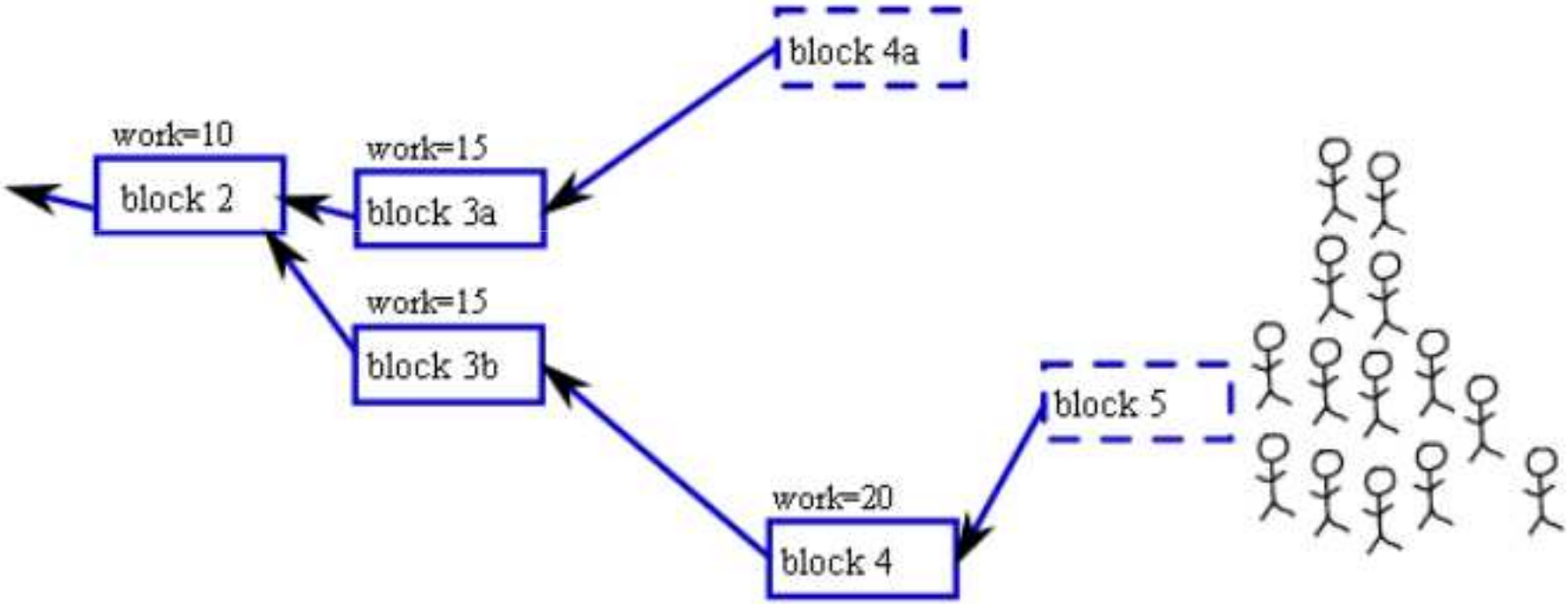
Fork – Miners Mine On Both Branches



Longest Chain Rule

[criticised in our paper]

"1 ASIC 1 vote"



51% Attacks

Cryptome Renamed My Paper:

CRYPTOME

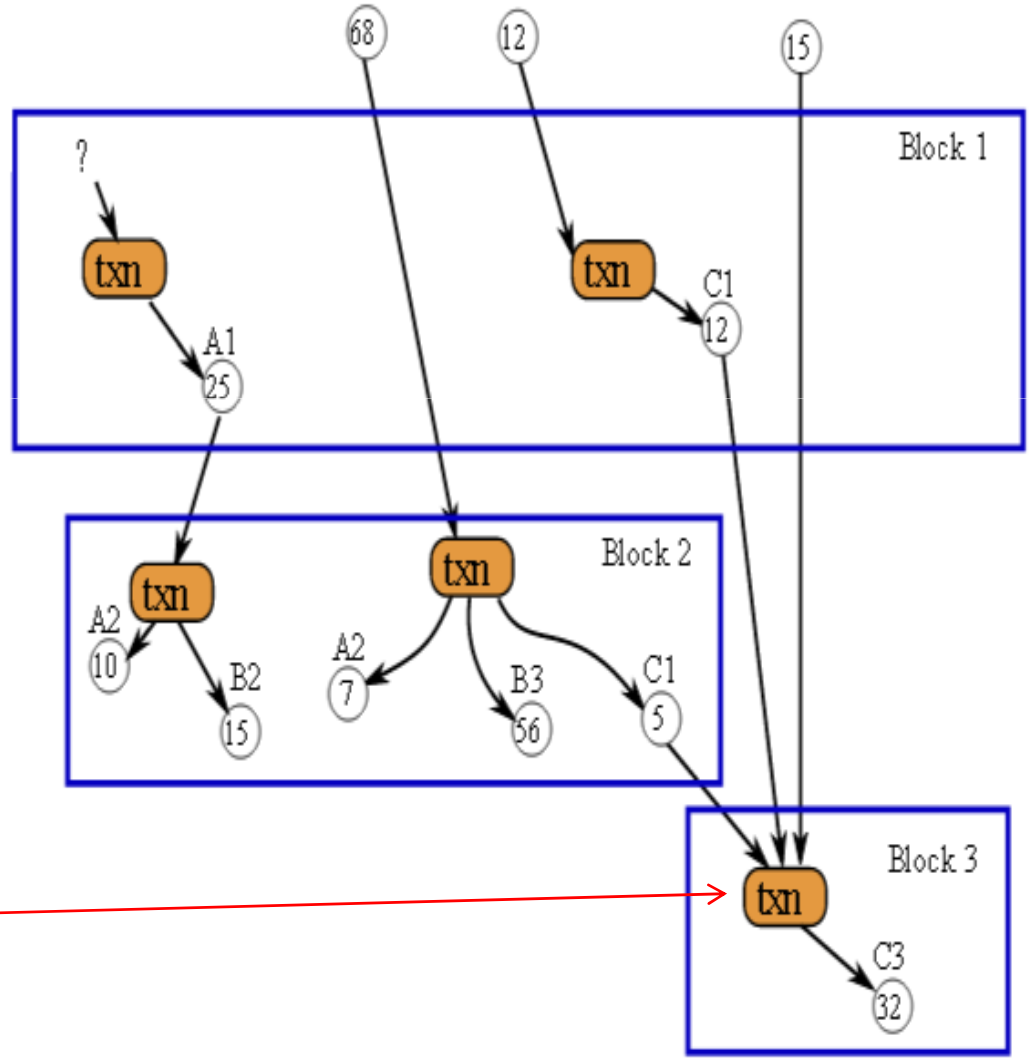
Donate for the Cryptome Archive of over 81,300 files from June 1996
key. (Local search temporarily disabled, use Google)
Bitcoin: 1P11b3Xkgagzex3fYusVcJ3ZTVsNwwnrBZ

http://cryptome.org/2014/05/bitcoin-suicide.pdf ??????????

=> Actually I show that quite possibly
bitcoin is EXEMPT from destruction [natural monopoly].

=> Whatever is Bad with bitcoin is
even worse with most alt-coins.

Cancel A Fresh Transaction?



Cancel this?

Can Sb. Cancel A Transaction?

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

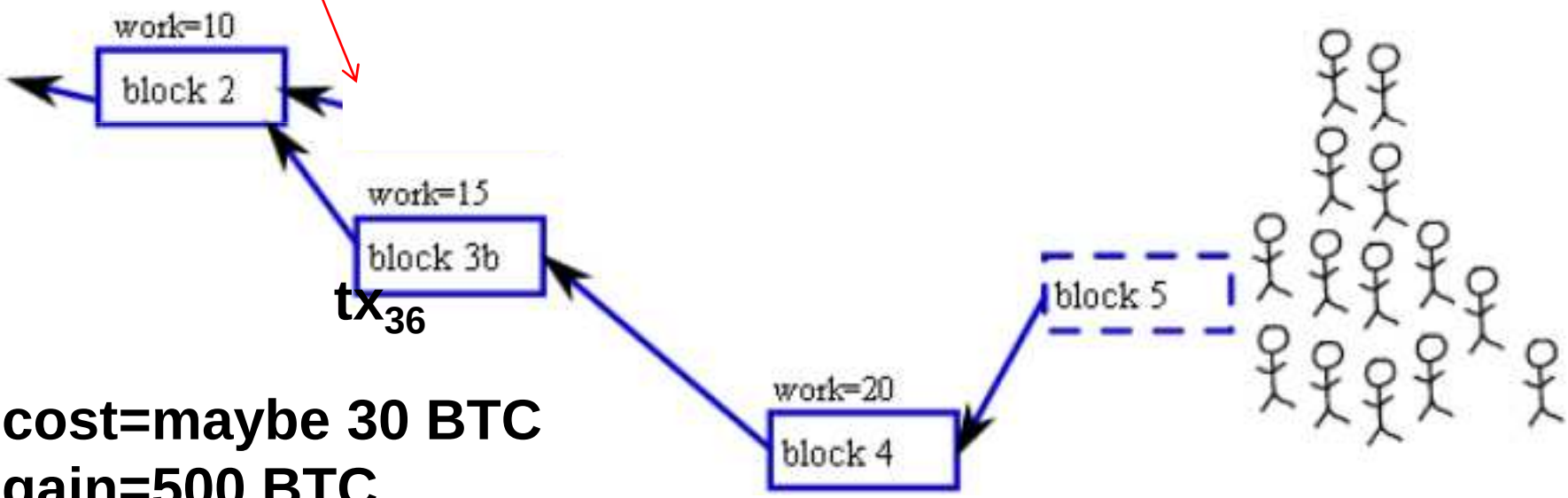
Very expensive, race against the whole network (the whole planet).

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 solo miners.

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)

51% -
Blunders Mistakes Misunderstandings

Is it a 51% Attack?

51 % attacks:

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

- almost nobody gets it right ever… including Sathoshi

Satoshi About 51%

Amazing level of confusion already in Satoshi writings:
in Section 6 of Satoshi paper we read that:

"The incentive[like 25 BTC] may help encourage nodes to stay honest.

If a greedy attacker is able to
assemble more CPU power than all the honest nodes,

he would have to choose between using it

- to defraud people by stealing back his payments,
- or using it to generate new coins. → **Q: who would own these new coins?**

He ought to find it more profitable to play by the rules,

such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

51% and the Longest Chain Rule

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:

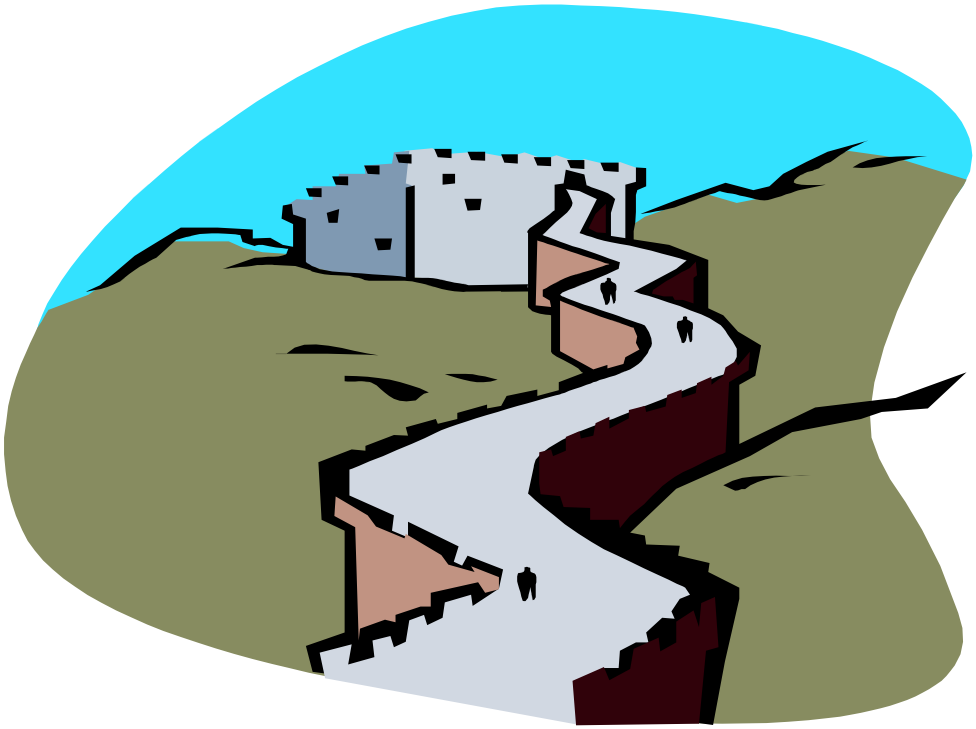
- Which block is paid (10 minutes)
- Which transactions are accepted (every second)

Violates the principles of

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

=> Unnecessary instability and slow transactions…

More Hash Power => More security?



THIS IS MISTAKEN

Bitcoin Mining

Money Out of Thin Air

Bitcoin vs. Klondike

2012-2014

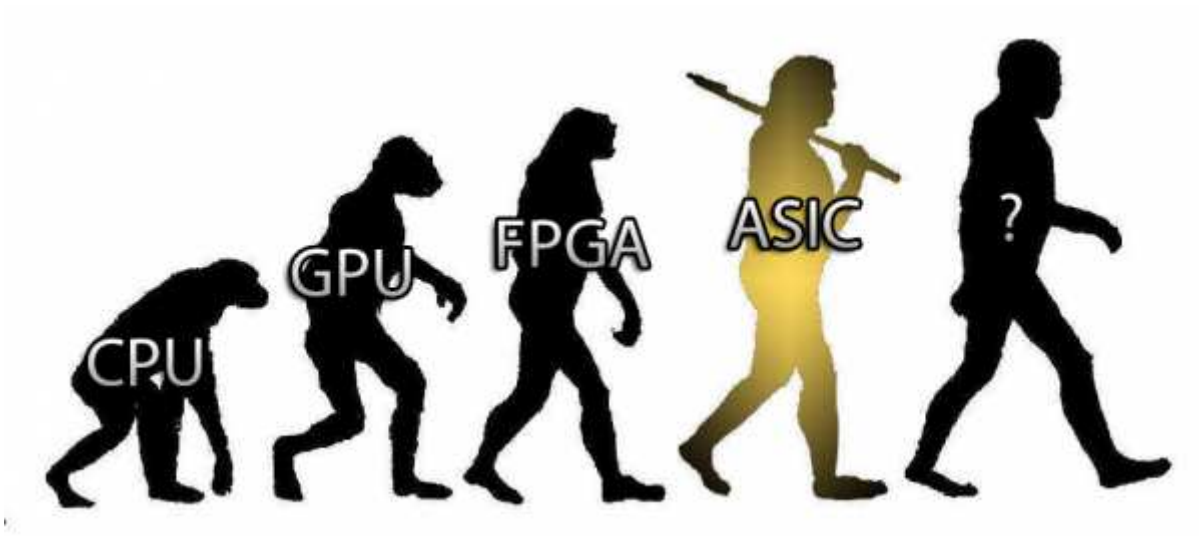
>100,000 miners

Most lost money

1896-1899
100,000 miners,
4,000 struck gold

BITCOIN MINER

Four Generations



Four Generations of Miners

1. CPU Mining

Example:

Core i5 2600K, 17.3 Mh/s, 8 threads, 75W

CPU = about 4000 W / Gh/s

Four Generations of Miners

2. GPU Mining

Example:

NVIDIA Quadro NVS 3100M, 16 cores, 3.6 Mh/s, 14W

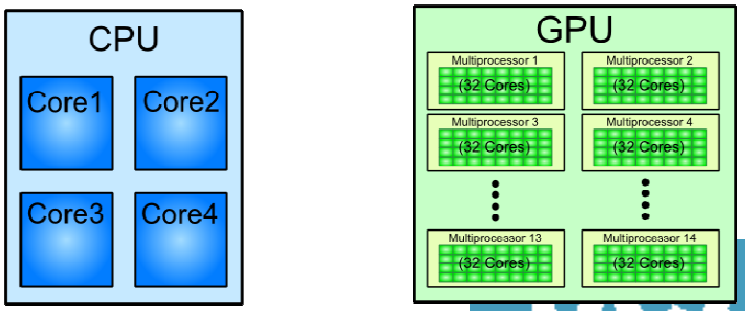
CPU = about 4000 W / Gh/s, in this case

GPU = about 4000 W / Gh/s, in this case

Who said GPU was better than CPU?

Not always.

CPU/GPU Architecture Comparison



Four Generations of Miners

3. FPGA Mining

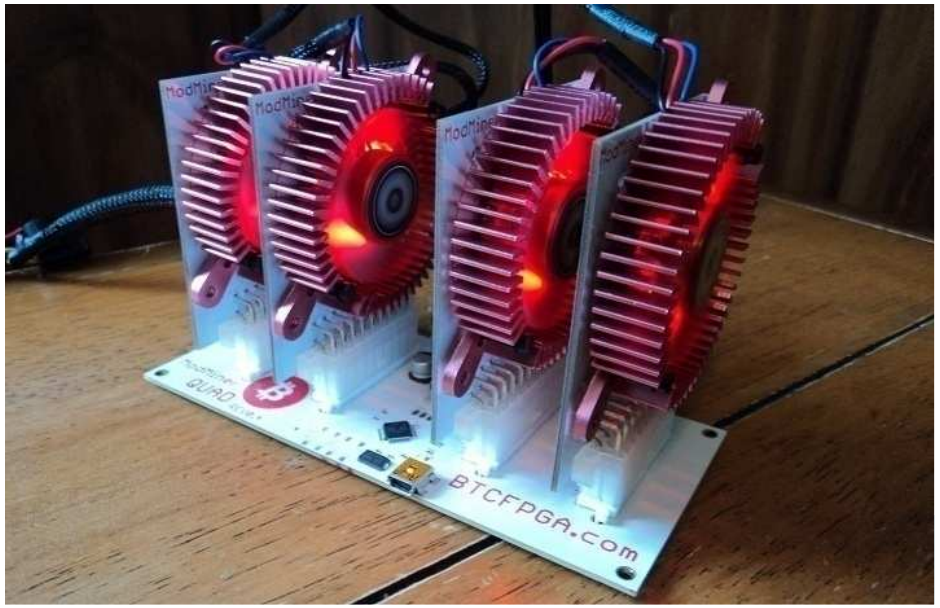
Example:

ModMiner Quad, 4 FPGA chips, 800 Mh/s, 40W

CPU,GPU = about 4000 W / Gh/s

FPGA = about 50 W / Gh/s

100x less energy.



Five Generations of Miners

4. ASIC Miners

CPU,GPU = about 4000 W / Gh/s

FPGA = about 50 W / Gh/s

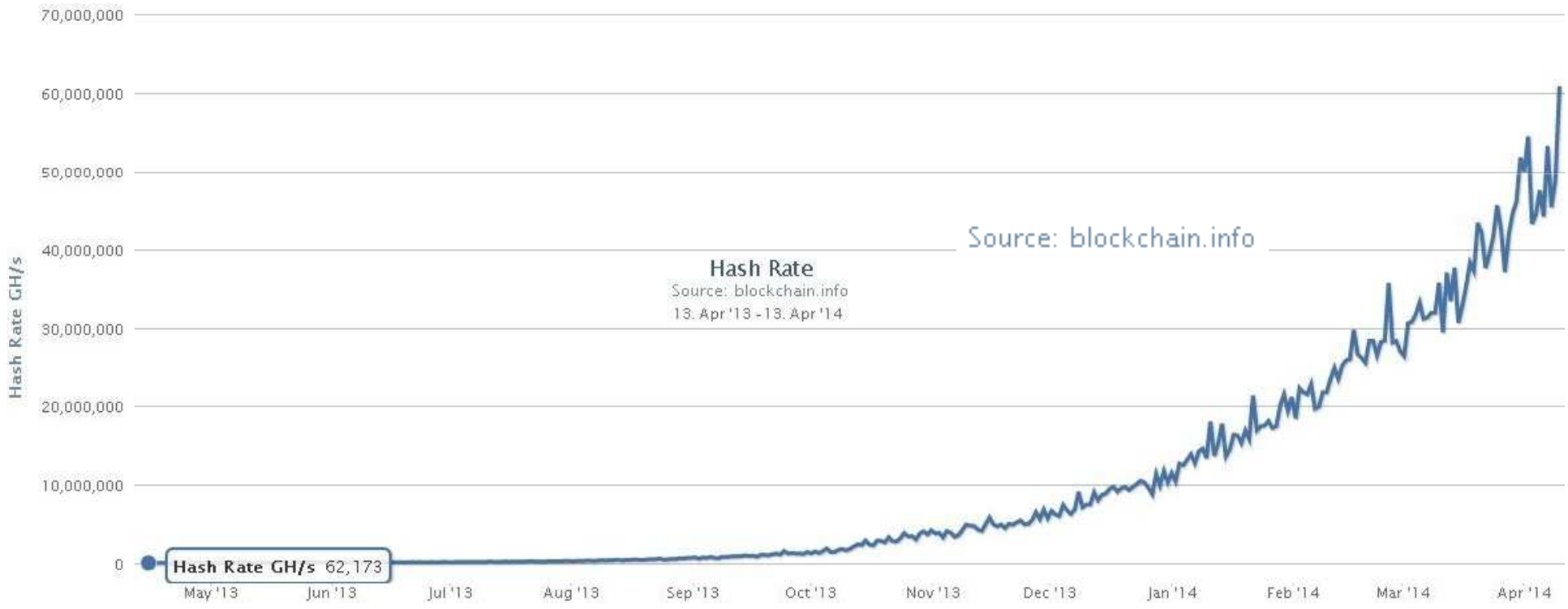
ASIC = now down to 0.35 W / Gh/s

Overall we have improved the efficiency 10,000 times since Satoshi started mining in early 2009…

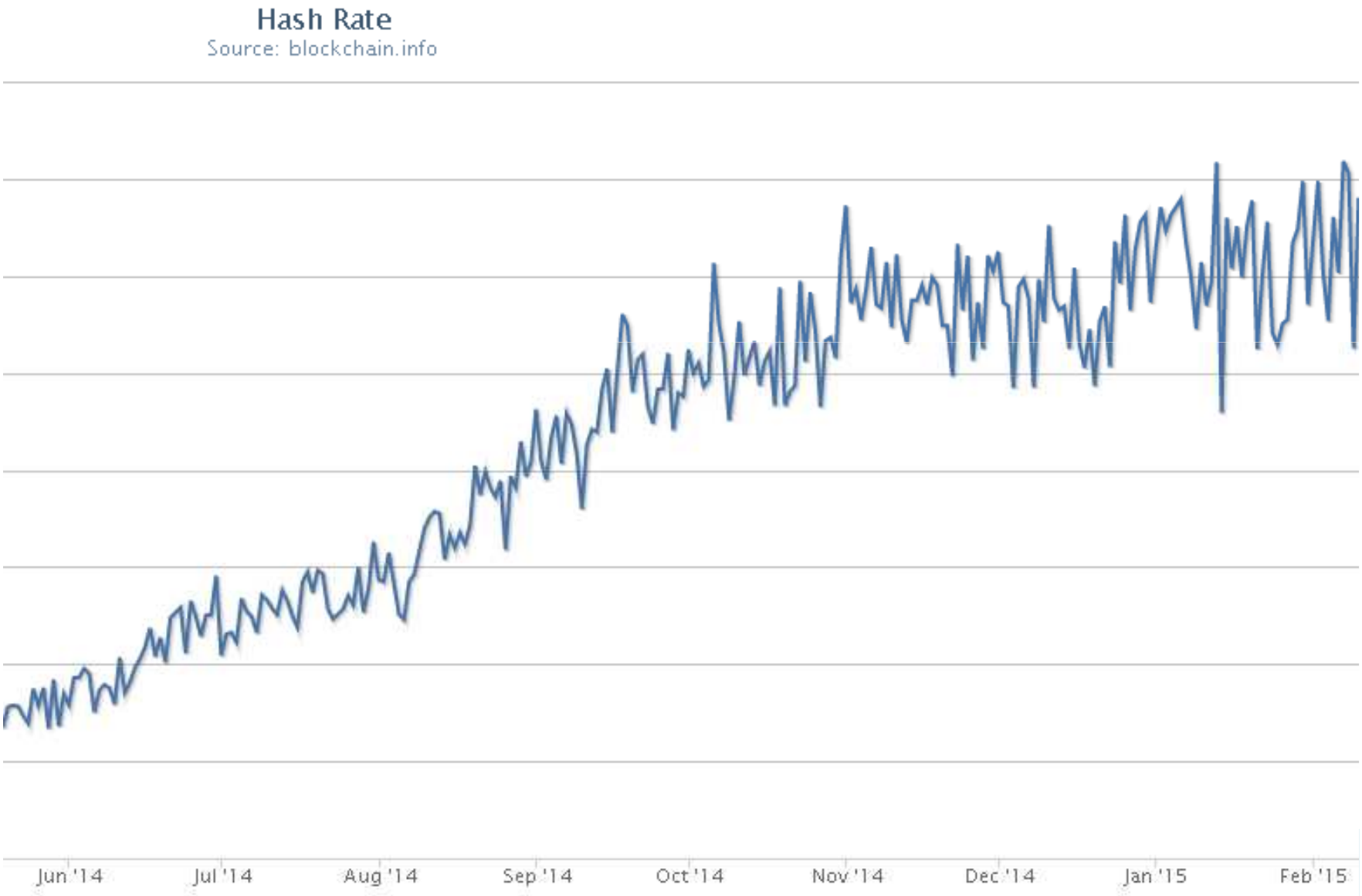
Like 1000% per year improvement.

Hash Rate - Doubled Nearly Every Month!

1000x in 1Y



Jan 2015: Peak Reached

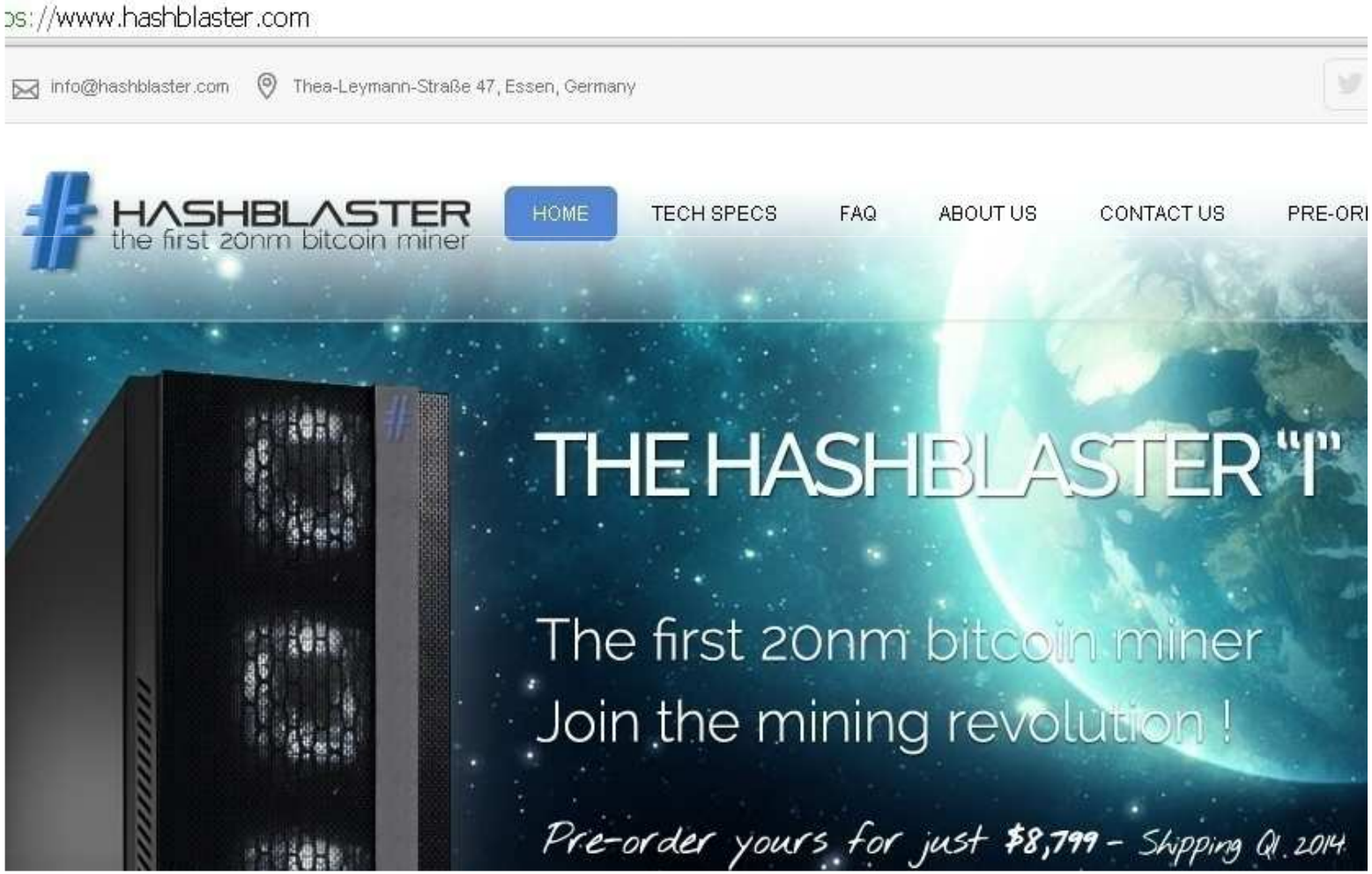


Criminal Scams

By consumers, for consumers...

Ripoff Report®

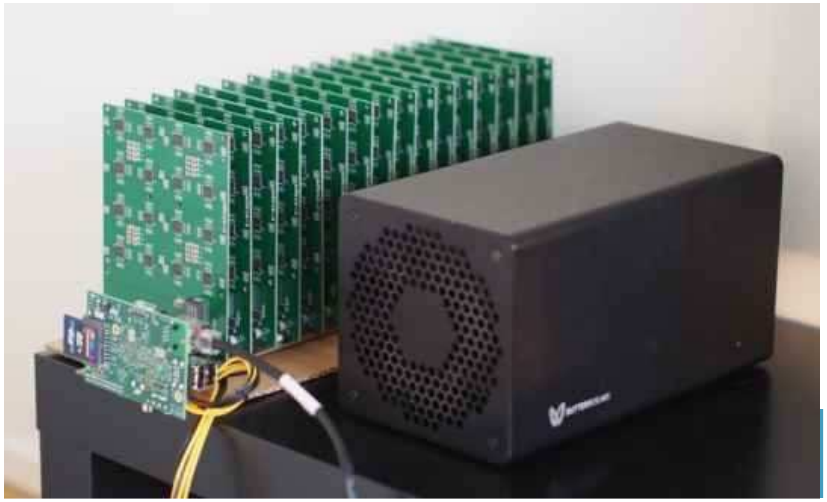
See bitcoinscammers.com



UCL

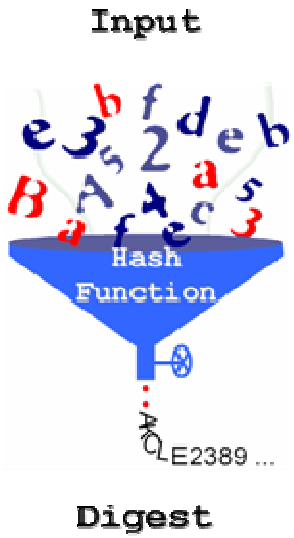
Total Cost? About 2.0 Billion USD

Extremely few people made a profit.

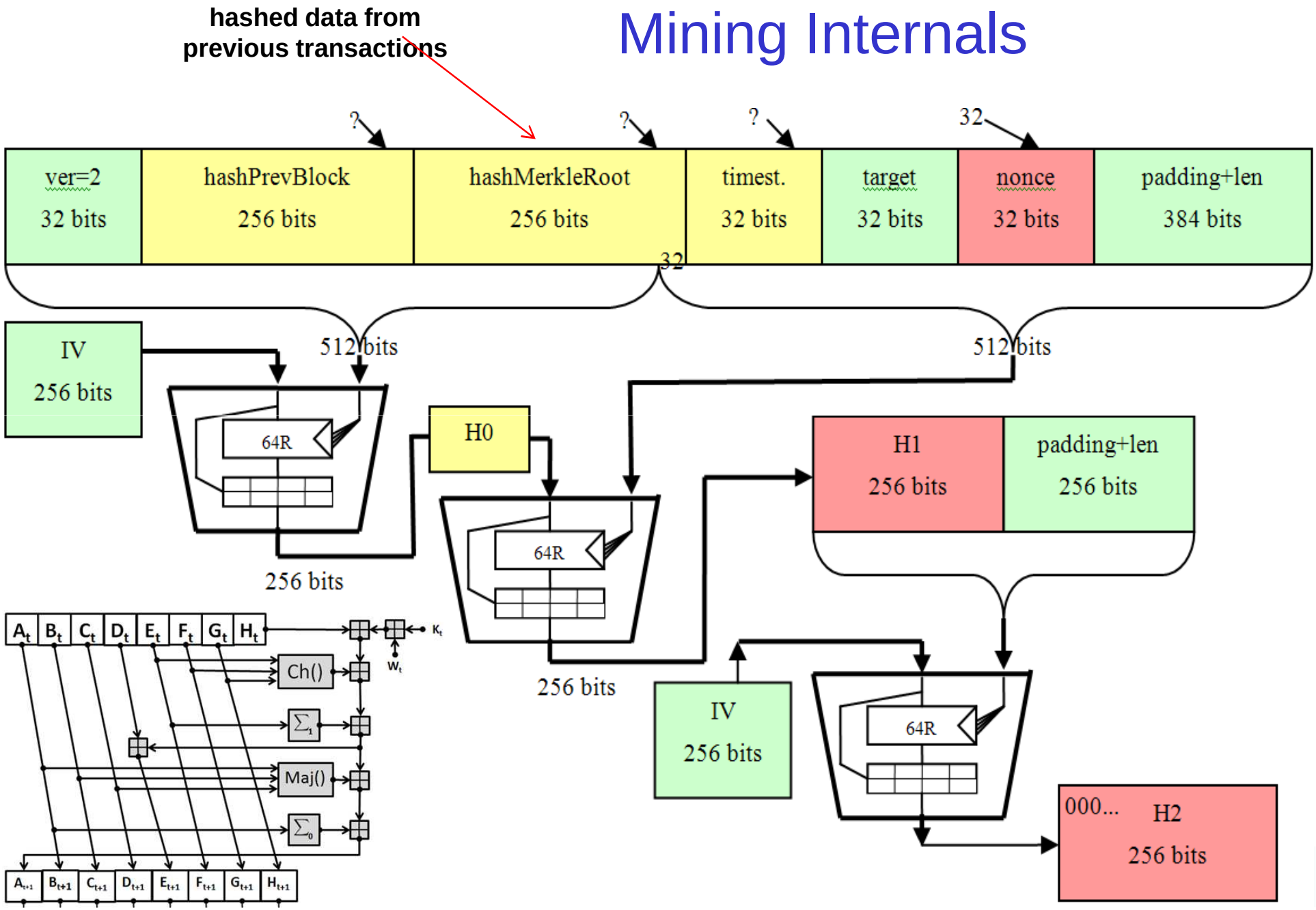


Bitcoin

And Hash Functions



Mining Internals

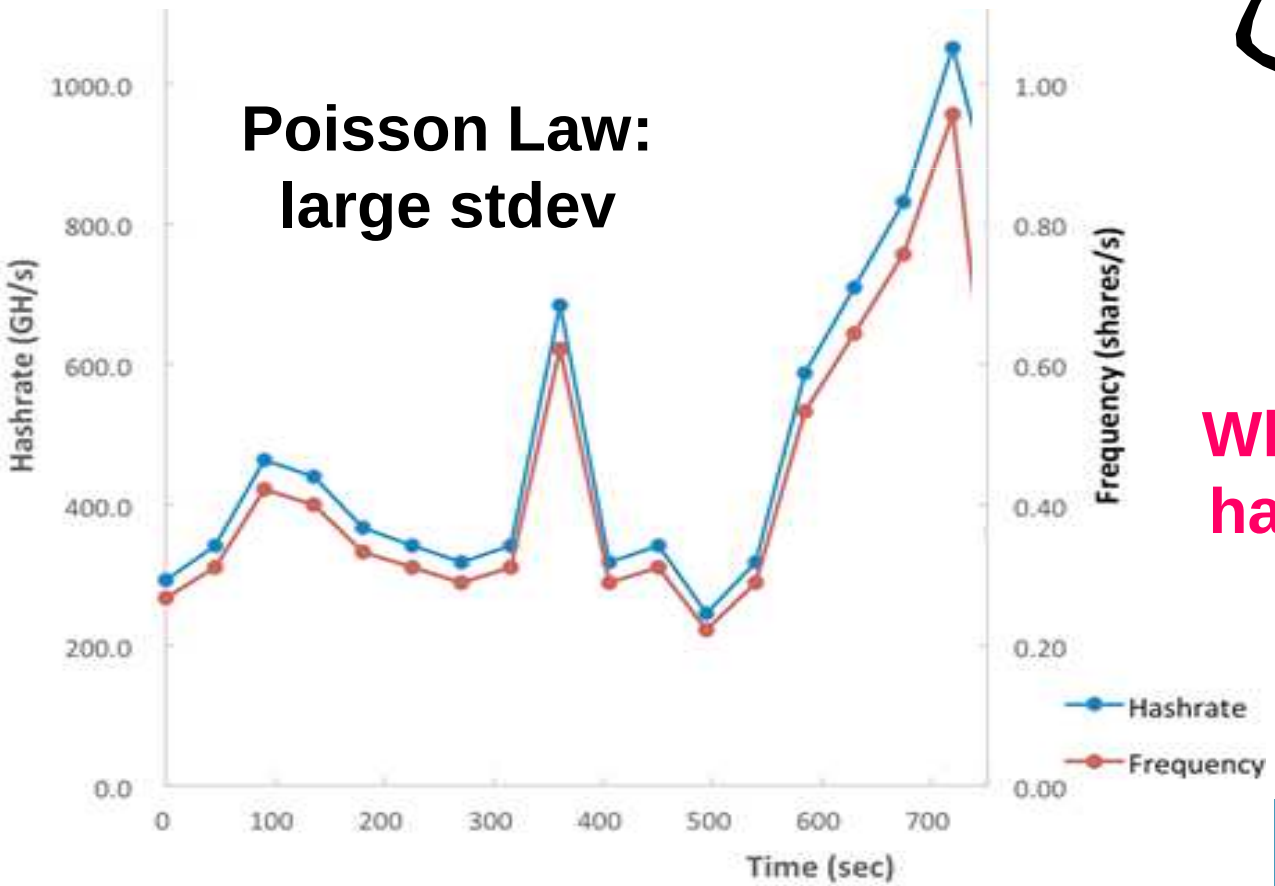


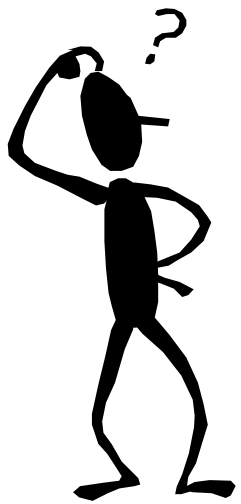
Mining In Pools

Why Pools?

Reason 1. To smooth the gains: Instead of waiting 1 year to get 25 BTC, why not get a little money every day?

Reason 2. Huge Incertitudes:





What is my hash rate?

What Are Pools?

- A group of small/larger miners who work together. Also protects their anonymity, also a social dimension:
- Single point of failure: pool servers.
  - can break down, miners will lose millions of dollars.
  - can attack the network (for example filter transactions which are accepted).

Major Pools In Existence

Miners tend to flock to the largest pools.

One pool has in 2014 reached 55%.

Feb 2015:

- Discus Fish: 20.9%
- GHASH.IO: 10.11%
- BTCChina: 7.64%
- 1LH3QtVjrQmK: 6.97%
- KNC: 5.17%
- Slush: 4.49%
- 1FeDtFhARLxj: 3.15%

10 large pools control 75%...

Pools Operation

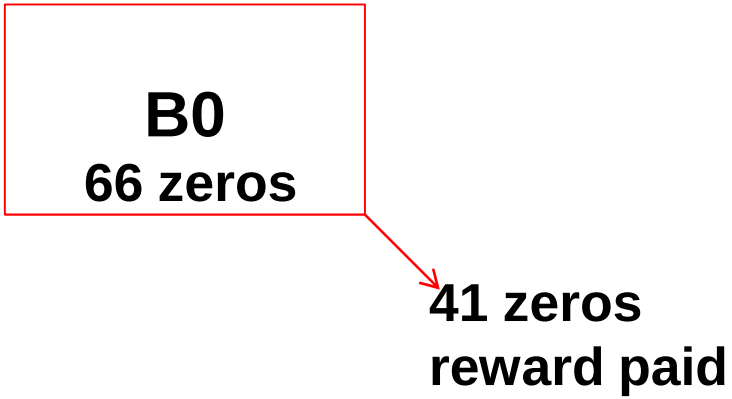
Question: but is there a “fair and secure” implementation?

Answer: Probably There Isn’t.
There is already ample literature on this.

Bitcoin Share

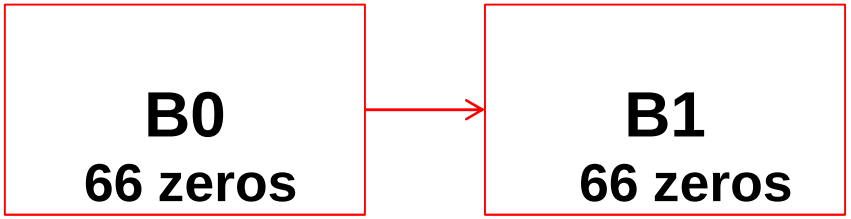
A proof of effort: allows one to be paid.

=def= A hash starting with 32 zeros (one in 2^{32} hashes).



much later, after some 2^{25} shares have been found…

66=41+25



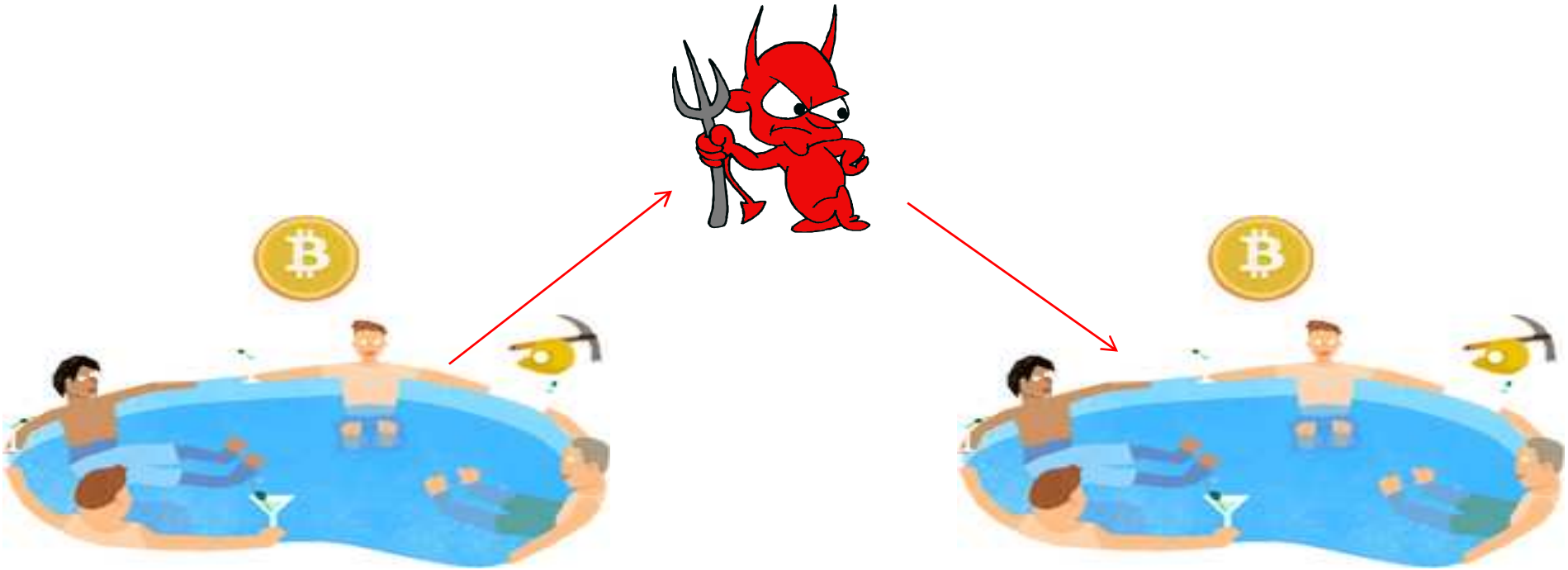
new block

**Dupe Shares

Apparently in certain pools it does happen that 2 people produced the same share.

Short answer: Pools should be designed in such a way that it does not happen…

Pool Attacks



Block Withholding Attacks

Cf. Nicolas Courtois, Lear Bahack:

On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency http://arxiv.org/abs/1402.1718

On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency

Nicolas T. Courtois
University College London, UK

Lear Bahack
Open University of Israel

***Abstract*—Bitcoin is a "crypto currency", a decentralized electronic payment scheme based on cryptography. Bitcoin economy grows at an incredibly fast rate and is now worth some 10 billions of dollars. Bitcoin mining is an activity which consists of creating (minting) the new coins which are later put into circulation. Miners spend electricity on solving cryptographic puzzles and they are also gatekeepers which validate bitcoin transactions of other people. Miners are expected to be honest and have some incentives to behave well. However. In this paper we look at the miner strategies with particular attention paid to subversive and dishonest strategies or those which could put bitcoin and its reputation in danger. We study in details several recent attacks in which dishonest miners obtain a higher reward than their relative contribution to the network. In particular we revisit the concept of block withholding attacks and propose a new concrete and practical block withholding attack which we show to maximize the advantage gained by rogue miners.**

Keywords: electronic payment, crypto currencies, bitcoin, bitcoin mining, mining pools, game theory

idea that – maybe– we do not need trust and good reputation. Neither we would need regulation, legislation, supervision, policing of fraud etc. All the things which are absolutely necessary for the traditional financial institutions to function. Instead bitcoin takes a truly and radically different approach. It is an attempt to build a financial infrastructure based on entirely new premises. A sort of peer-to-peer financial anarchy run by people who trust no one.

B. The Cryptographers' Dream

The main proposition is something which we frequently see in cryptography. We call it a cryptographer's dream: a dream about the world which functions with participants which do not see each other, do not trust each other a lot, and yet are able to somewhat function and achieve some sort of "secure function" or prevent fraud from being committed. An attempt to build systems which remove the necessity of having trusted

Breaking News!

On 13 June 2014 it was reported that

a large-scale block-withholding attack

as described in our paper (or a variant), see Section XI-A

was executed against the mining pool Eligius

- probably run by large miner earning millions of dollars
- OR run by a mining pool without knowledge of individual miners

see

https://bitcointalk.org/?topic=441465.msg7282674

Many Researchers Get It Wrong:

In the same blog post we read:

"the attacker does not gain any direct benefit by performing the attack".

https://bitcointalk.org/?topic=441465.msg7282674

Cornell researchers claim that same in their blog post written on the same day: "the attacker doesn't gain anything from this behavior, either; it's purely destructive".

Source: http://hackingdistributed.com/2014/06/13/time-for-a-hard-bitcoin-fork/#sthash.uc9I6ink.dpuf

Again the attack is trivially profitable as shown in our paper and if 186,000 USD was lost to honest miners, probably half of this sum was earner by the attackers (like 150 BTC profit) assuming they DID apply our optimal 50-50 strategy [see the paper].

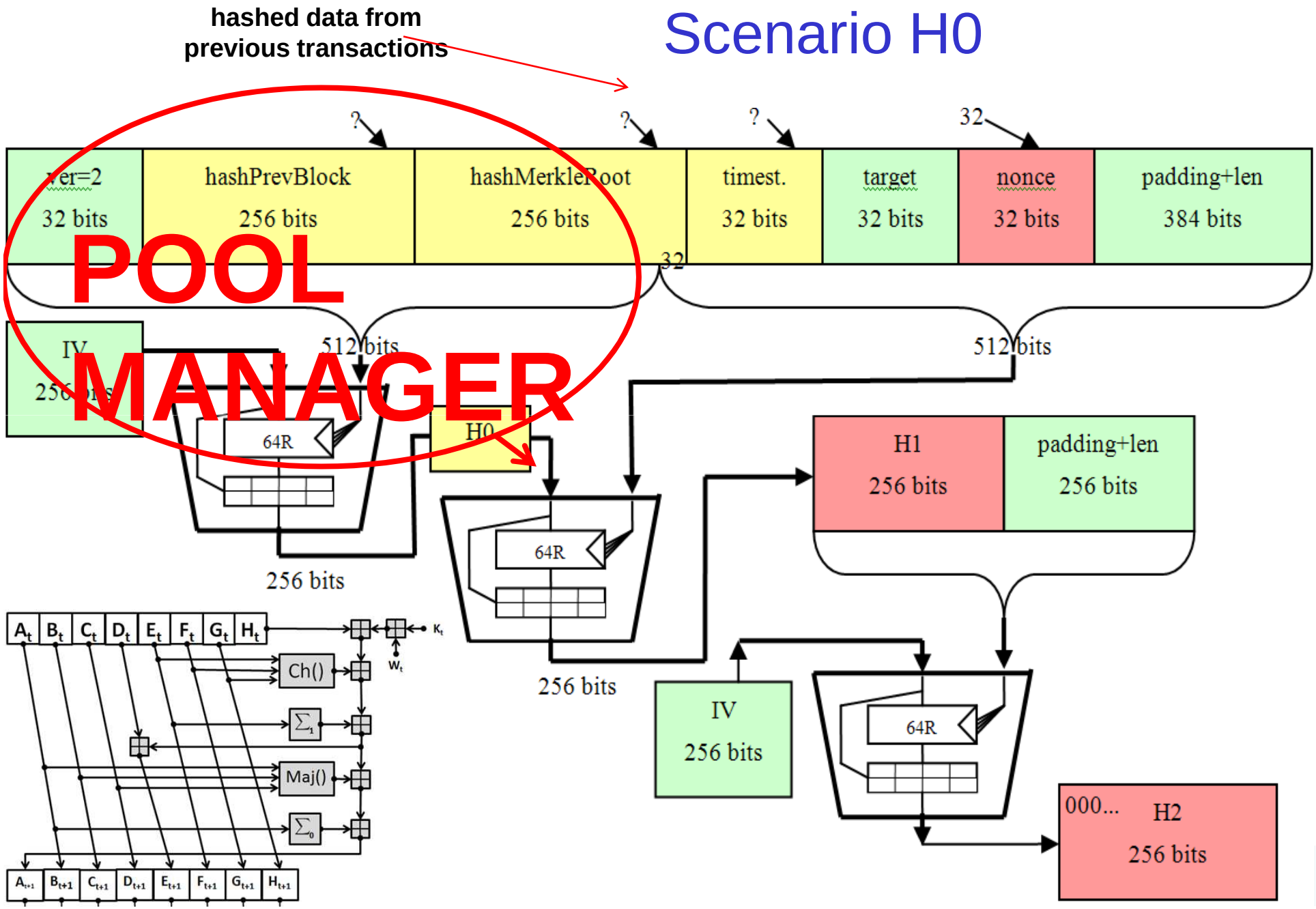
MITM Attacks?

Possible Goals

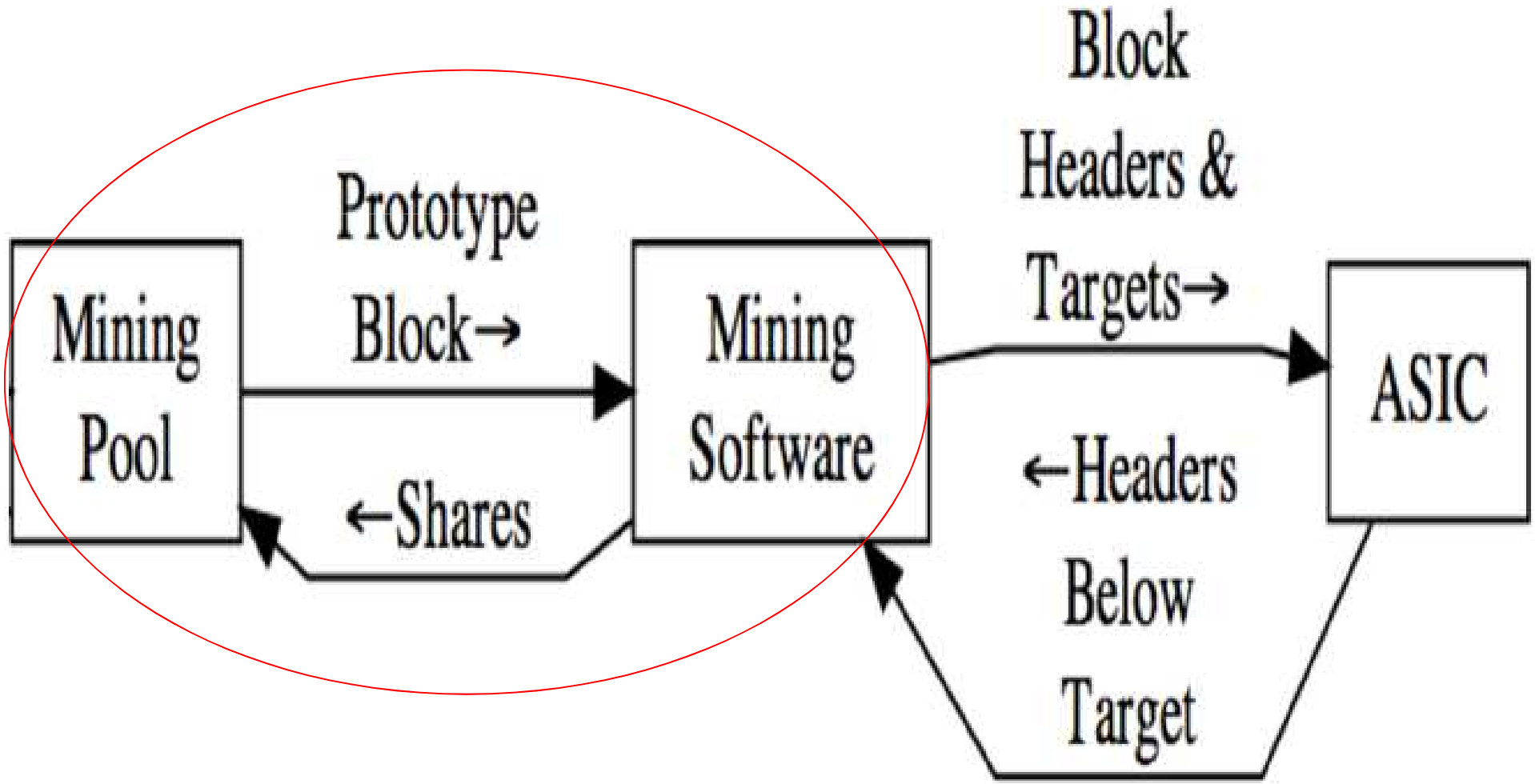
- abuse miners
- steal the money (harder)

There are many other possible goals: e.g. block withholding attacks etc.

Scenario H0


hashed data from
previous transactions
?
?
?
32
ver=2
32 bits
hashPrevBlock
256 bits
hashMerkleRoot
256 bits
timest.
32 bits
target
32 bits
nonce
32 bits
padding+len
384 bits
32
POOL
MANAGER
IV
256 bits
512 bits
512 bits
64R
H0
256 bits
64R
256 bits
H1
256 bits
padding+len
256 bits
IV
256 bits
64R
000...
H2
256 bits
Ch()
Maj()

Stratum Protocol [2012]



Stratum: Power Shift [After December 2011]

With Stratum

“miners cannot choose Bitcoin transactions on their own”.

Source: The designer of Stratum: https://mining.bitcoin.cz/stratum-mining

- The author claimed that

"99% of real miners don’t care about transaction selection anyway“

- Key point in history where bitcoin became more centralized AND miners lost control of what they mine

Server Work Communication (mining job)

(Eligius)

Server: {"params": ["1403009309 11666",
"292ad15f13fed14a9a1316b9f52b9d3a234a2f572ab8bd210000000000000000",
"0100000001000000000000000000000000000000000000000000000000000000000000000000000000ffff
ffff52038bac040d00456c69676975730053a0391dfabe6d6d245d64a852df57ba3cf5c24b53e459a
b9dba49e37f724a70637956ee3754d3ce0400000000000000002f737332332f00",
"ffffffff1a1804400000000000001976a9143810f95cc7d5d9b06c378244172aa8311681f1a488ac568
94000000000001976a91460876095942498c23f4071d615db8982550d60f788ac2c994000000000
001976a9144ebf00154078a5ee78599adb4a82ce3b75709f5688acef084000000000001976a91429
...00001976a9148ec06cc970e54b5dfe10a90c1eff2232d2300d1b88ac1d074100000000001976a9
14e40a50aef7f788ac81d14000000000001976a914e078ecbed20e721047e5e2603886c5ae4f5ffae
788ac6667ae83000000001976a914ecf0dfe07072afaed4135e99c70072cce2235a7f88ac01000000
000000001976a9145399c3093d31e4b0af4be1215d59b857b861ad5d88ac00000000",
["68d4a3ad27c5d28db7822fec92e7cac4df87fe5ac10da74b1d52e01c7da4ce6a",
"56915e09578a0de92d75ba99cf62a8efc349522aeb22a3666c7bfda46a4d1d1d",
"c2f5fb89e3c57661e24dca08e9c7136ecfcceaefcf0f05dc835c04a3fa0d844d",
"030caee1ca788183fff3a36ace4bb349d8c2b3ed8179a8645cb6c5123a2517bb",
"cf21863105d786b879fd4f8dcadac718b4463c92eb6c146babf8bdc1a9ac2df8",
"c4f6d1fd9eff04c195c60bbd313361249e78615d3ca4e8aa429450aa5fa597a4",
"cf30725051d4ea58b092e96296021393fcc3d3706b597b9eb58866fc994f40f0",
"8b8684e57f660235abe876ee5d1cd349d52f9b8cffa9588eb1327f8e00f4a2cd"], "00000002",
"185d859a", "53a0391d", false], "id": null, "method": "mining.notify"}

- timestamp
- prevhash
  makes the attacks detectable
- coinbase1
- coinbase2
- merkle branches 8-11 observed
- version
- nbits
- ntime
- clean jobs

4a. Worker Submissions (submitting a share)

<= {"params": [“…my payout address…..", "1411838942 347213", "e1210000", "5426f3de", "a14b7d5f"], "id": 3012184, "method": "mining.submit"}

- address of the miner
- time stamp
- ExtraNonce2
- ntime
- nonce
- job ID

genuine example, real data!

Q: How does the pool know it is correct?

4a. Worker Submissions (submitting a share)

<= {"params": [“…my payout address…..", "1411838942 347213", "e1210000", "5426f3de", "a14b7d5f"], "id": 3012184, "method": "mining.submit"}

- address of the miner
- time stamp
- ExtraNonce2
- ntime
- nonce
- job ID

genuine example, real data!

Q: How does the pool know it is correct?

MUST RECOMPUTE THE WHOLE BLOCK!

Conclusion

- **The security of Bitcoin against 51% and double-spending attacks is beyond the scope of the strict open-source system and code created by the anonymous founder Satoshi Nakamoto.**
  - **Satoshi did not predict pooled mining.**

- **The content of the bitcoin clockhain depends on the Stratum protocol specified later [early 2012].**
- **this decision broke bitcoin,**
  - **it has become VERY HIGHLY centralized, 10 major pools control 75% of mining power. Miners have no control on the exact content of bitcoin blockchain.**

Bitcoin is NOT a decentralized system yet.