

Bitcoin Mining, Internals, Stratum Improvements and Attacks, Forks, 51%, Double Spending Attacks



Nicolas T. Courtois



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), <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) <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) <http://arxiv.org/abs/1405.0534>
- Nicolas T. Courtois, Pinar Emirdag and Daniel A. Nagy: [Could Bitcoin Transactions Be 100x Faster?](#) In proceedings of SECRIPT 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](http://eprint.iacr.org/2014/848), 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.

Introducing Bitcoin





Bitcoin In A Nutshell

- bitcoins 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
- 
- An illustration of a hand in a blue sleeve holding a blue pen, signing a yellow document. The document has some black scribbles on it. The entire illustration is surrounded by a pink starburst effect.
- 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

Miracle Of Bitcoin



Removes two pillars of money:

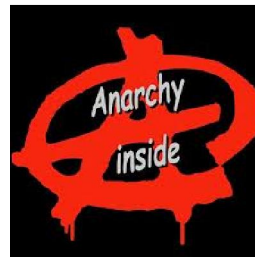
- “trust”

=> P2P self-regulation

<= self-interest?

- legal/government protection and policing

=> anarchy!



Citations

Bitcoin is:

- **Wild West** of our time [Anderson-Rosenberg]



Citations

- There is **no “undo” button** for sth. like bitcoin
[Mike Gogulski]



Krugman

- Bitcoin is ...
 - “the anti-social network”
- Paul Krugman,
Nobel price in economics



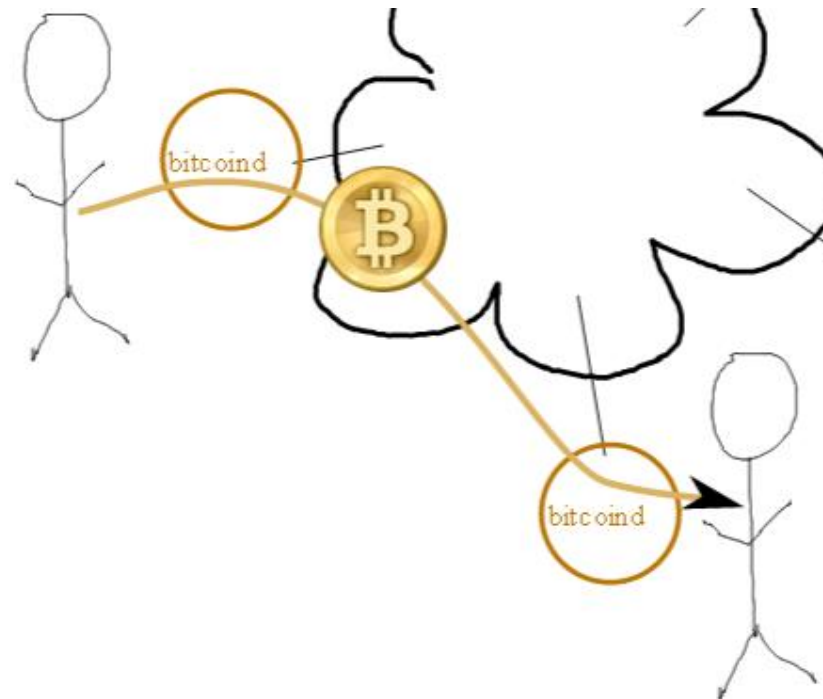
Who Is Evil?

- “Bitcoin Prevents Monetary Tyranny”
- Jon Matonis for Forbes
- “Just thinking about bitcoin makes you a better person” – Max Keiser

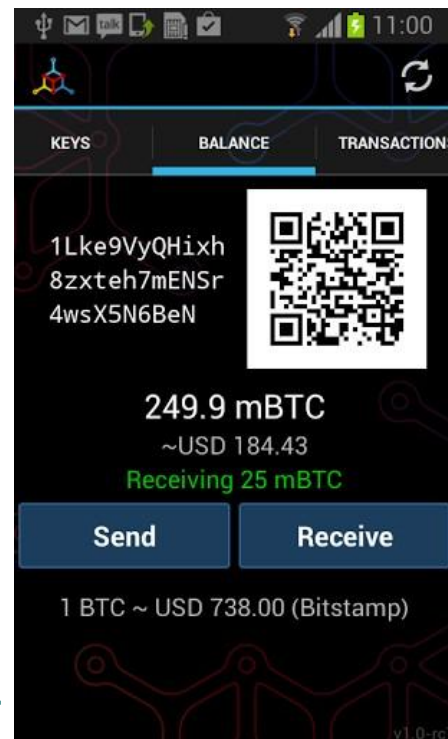
Money Transfer

To: 1K2CcfWYW5sBL2xSeQWxpcmjPCgoXdi36
Amount: 1.0 BTC

SEND



In Practice



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...



Download Bitcoin-Qt



Windows (exe)

~12MB



Mac OS X

~14MB



Windows (zip)

~16MB



Linux (tgz)

~16MB



Ubuntu (PPA)

~4MB




Source code

(GitHub)

Mobile Apps - Android





Bitcoin

SEND COINS

ADDRESS BOOK

BTC1.1163

= EUR55.7050

Your Bitcoin Address:

1KGe NiDw zH5N
rdwN ETj3 hQEx
wr5H MN9e FW

	balance	67.9065	Received	Both	Sent
CNY	rate	416.78	<div> <div></div> <div>Apr 6</div> <div>←</div> <div>1719Pmohr5Ck1dX6mQ9zYj4nTPnGD</div> </div>		
	balance	465.2653	<div> <div></div> <div>Apr 5</div> <div>←</div> <div>Beer with Lisa</div> </div>		
DKK	rate	328.56	<div> <div></div> <div>Apr 5</div> <div>→</div> <div>1Q4H8CY4FpnJ93SPbdz4Cqgv714KX</div> </div>		
	balance	366.7824	<div> <div></div> <div>Apr 4</div> <div>→</div> <div>Burger @ room77</div> </div>		
EUR (default)	rate	49.90	<div> <div></div> <div>Apr 4</div> <div>←</div> <div>1G9Hjz1JCUqnhNQmpxLhsVL6FD8Co</div> </div>		
	balance	55.7050			
GBP	rate	40.74	<div> <div></div> <div>Apr 4</div> <div>←</div> <div>Donation</div> </div>		
	balance	45.4794	<div> <div></div> <div>Apr 3</div> <div>←</div> <div>1FUgQeguKnVFavXYqKwYB7g4YKXJ4</div> </div>		
HKD	rate	506.94			

Are They Crazy?

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

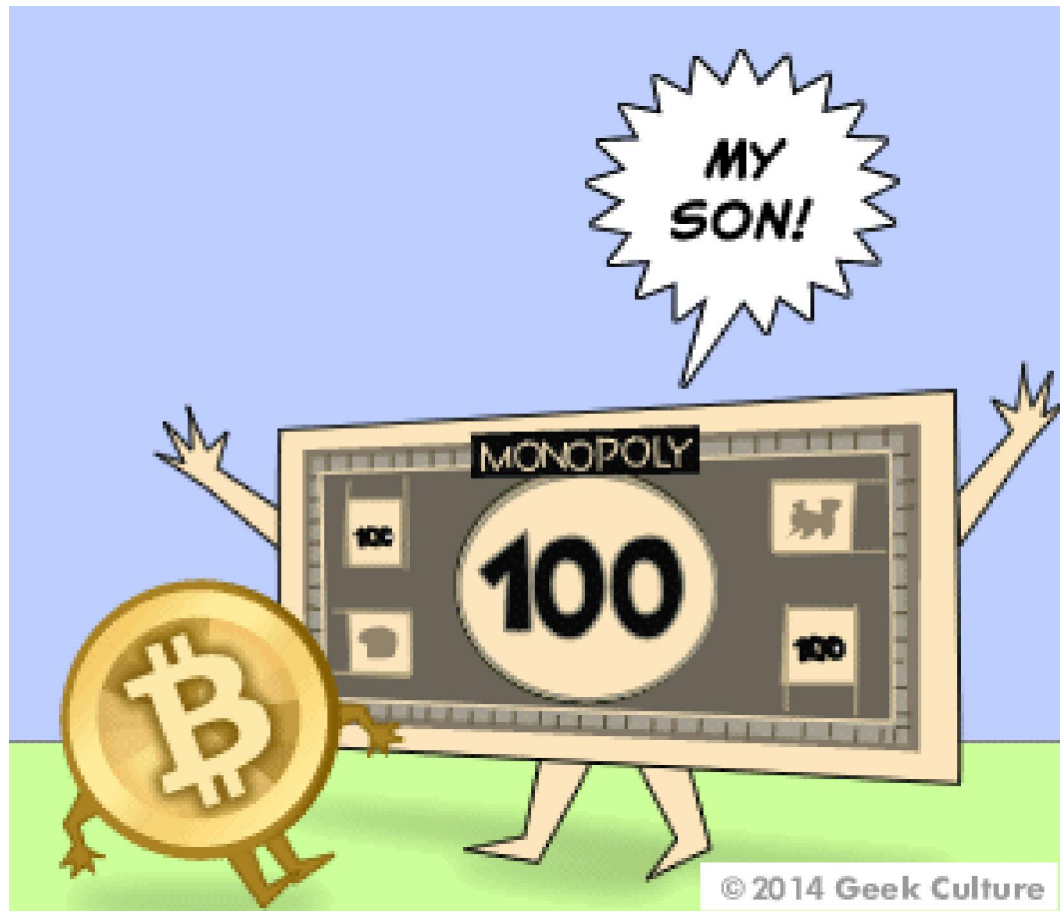
Question of:

- popularity
- trust

NO NEED TO TRUST ANYONE IN BITCOIN????

Play Money?

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



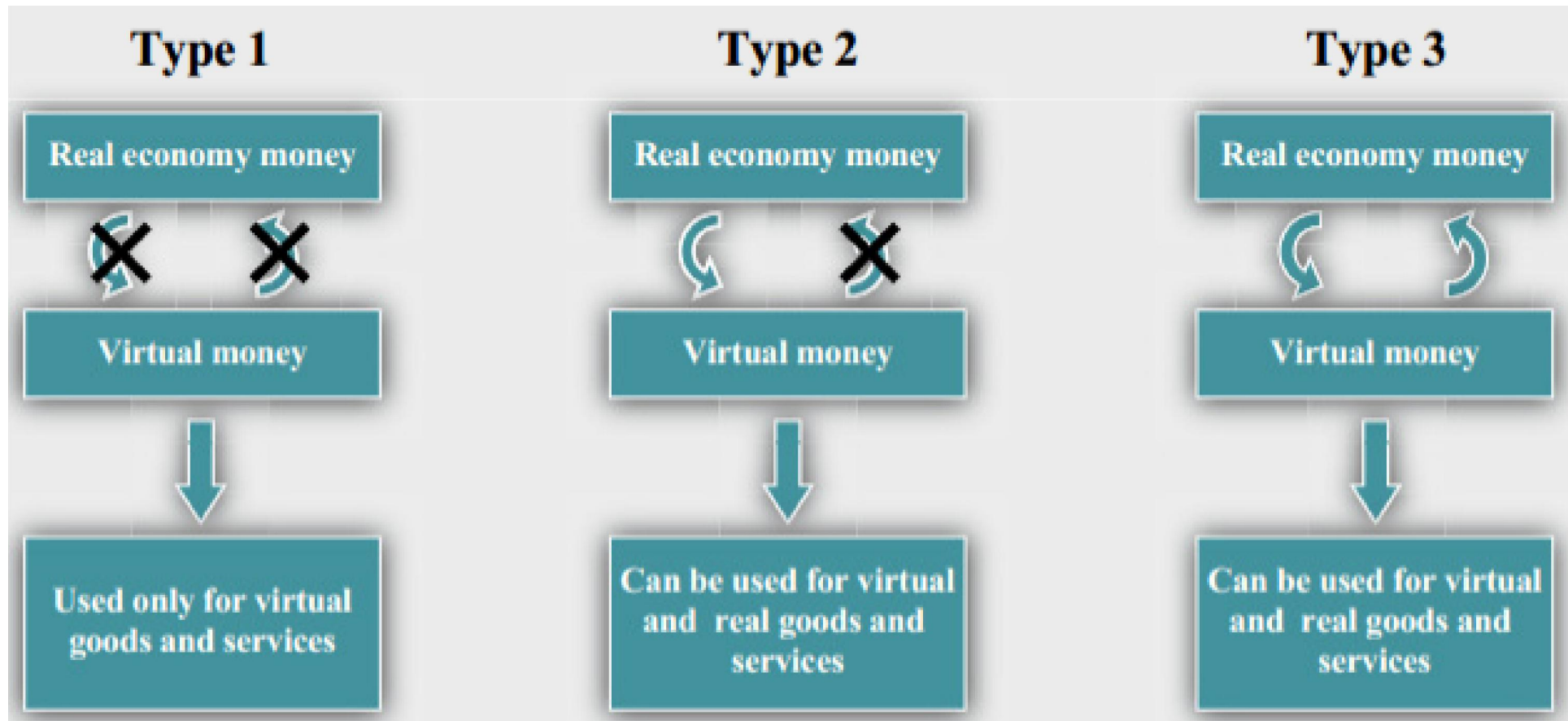
Types of “Virtual Money”

Source: ECB report, 10/2012

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



cf. Oyster...



Bitcoin=Freedom

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!] and forces finance to become more “transparent”

“Troubled” bitcoin [The Economist May 2014]
is certainly is here to stay

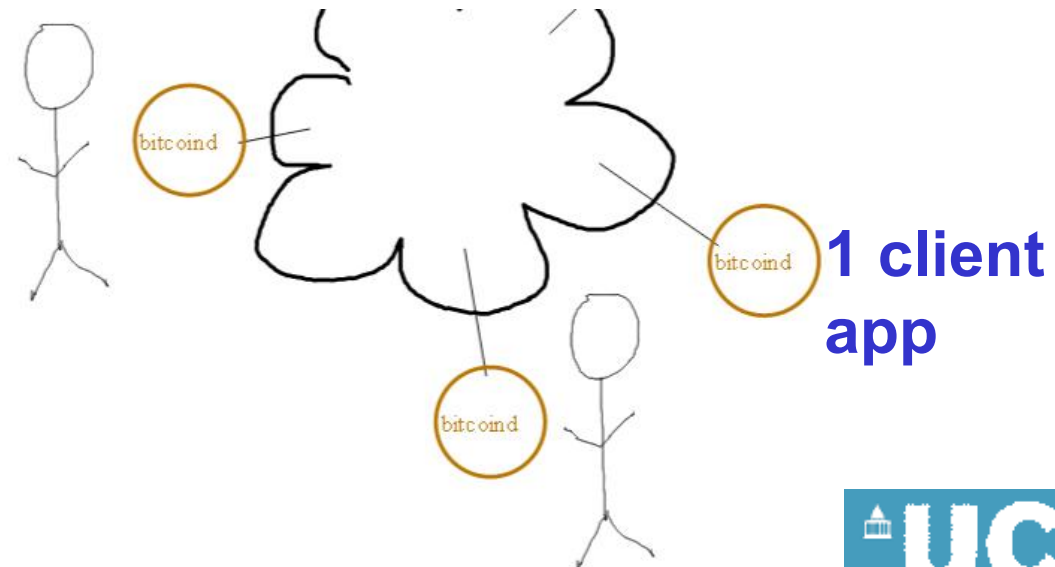
=> but now must face all sorts of competition and technical reforms [our work]

P2P Payment



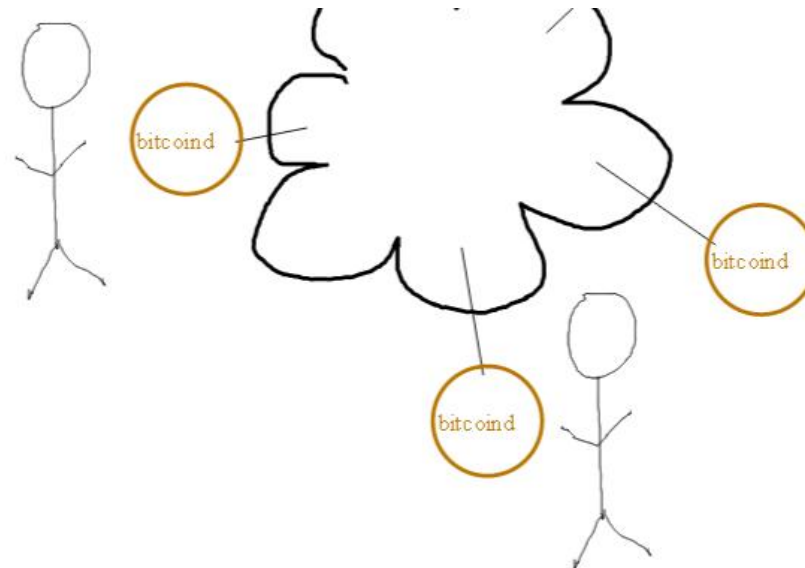
Bitcoin Network

- 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...



Bitcoin

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



Not written in stone

- Upgrade the software, change the spec:
 - people vote with their feet



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
- 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



*Scalability Issues

- Current bitcoin processes only 1-4 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 about 7 tr/sec
 - we are VERY close to exceed that, few months...

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".
 - about managing private keys

Wallets

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



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!

More Properties of Bitcoin



- **Scarce**, like gold (in fact worse than gold),
- **Divisible** into small pieces
 - 10 nBTC = 1 Satoshi = 1 / 100 million BTC

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) <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)



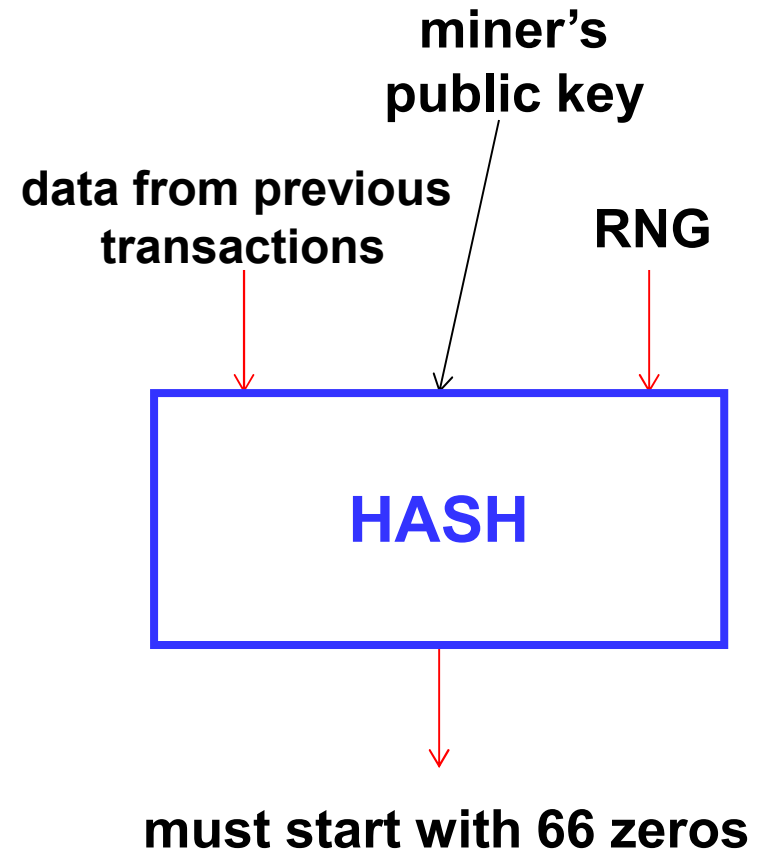
Bitcoin Mining

- 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:



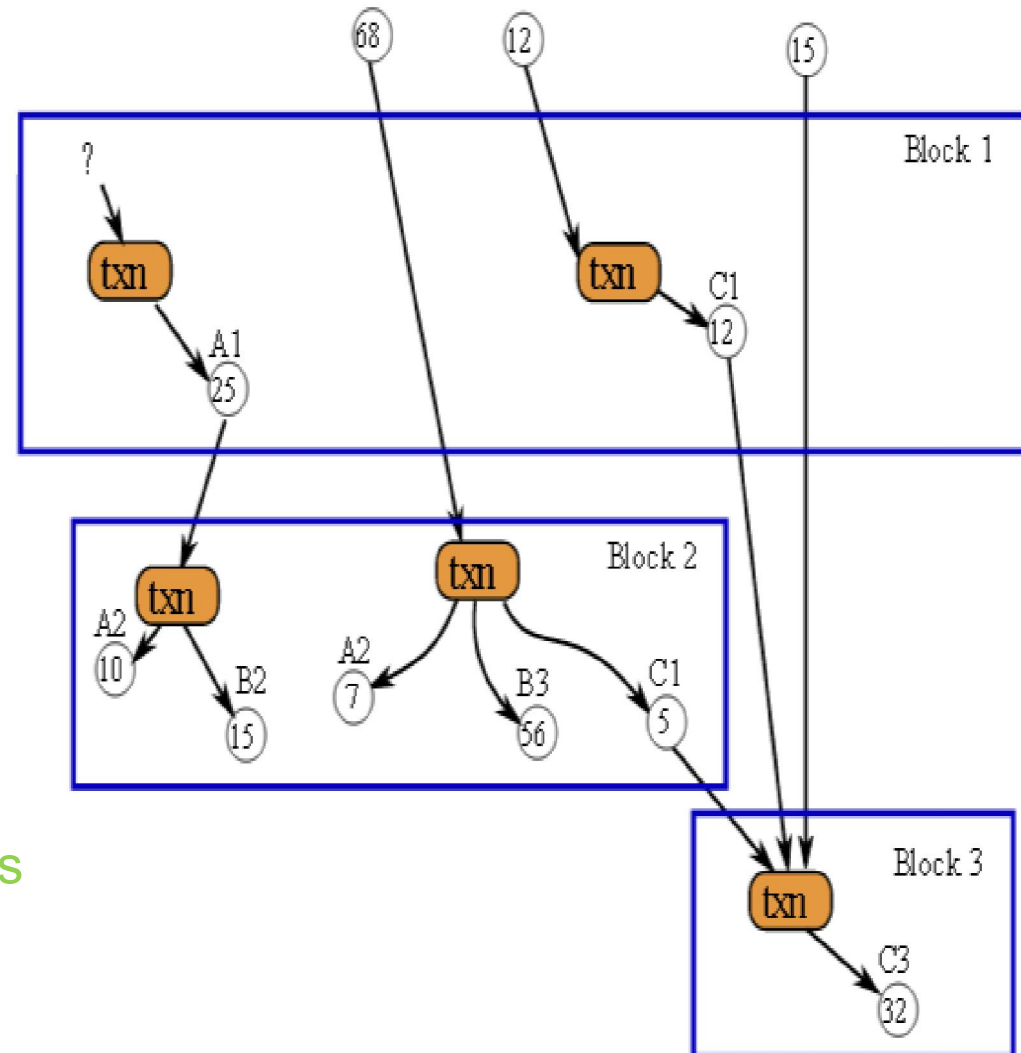
A transaction database
shared by everyone.

Also a ledger.

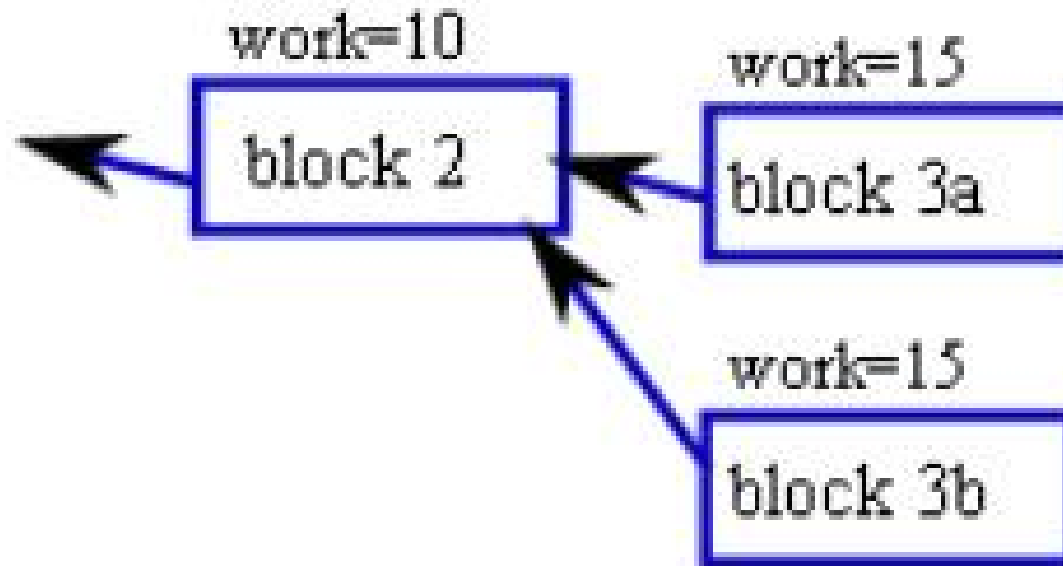
Every transaction
since ever is public.

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

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

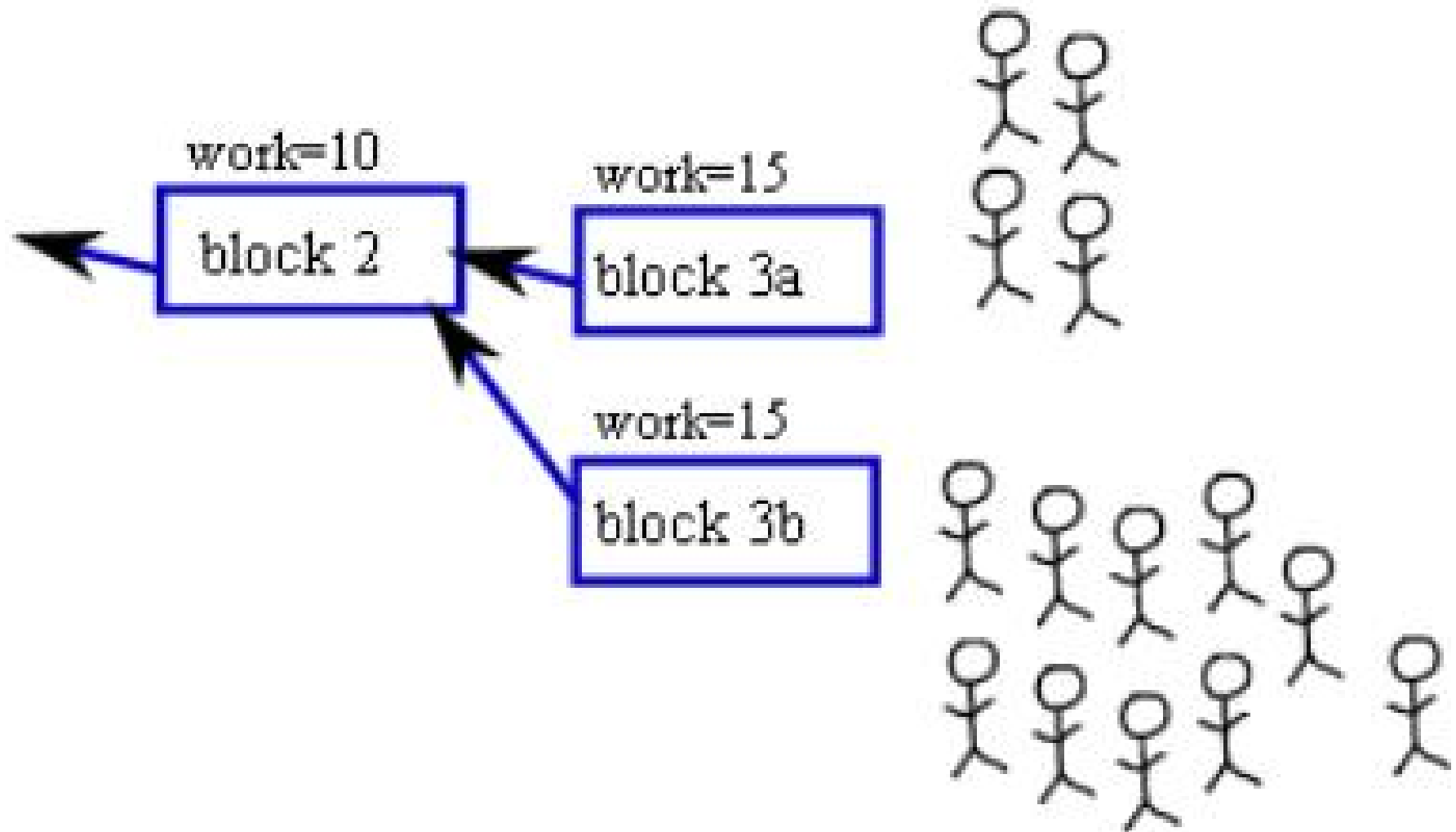


Fork – Hard To Avoid, 1% of the time



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%

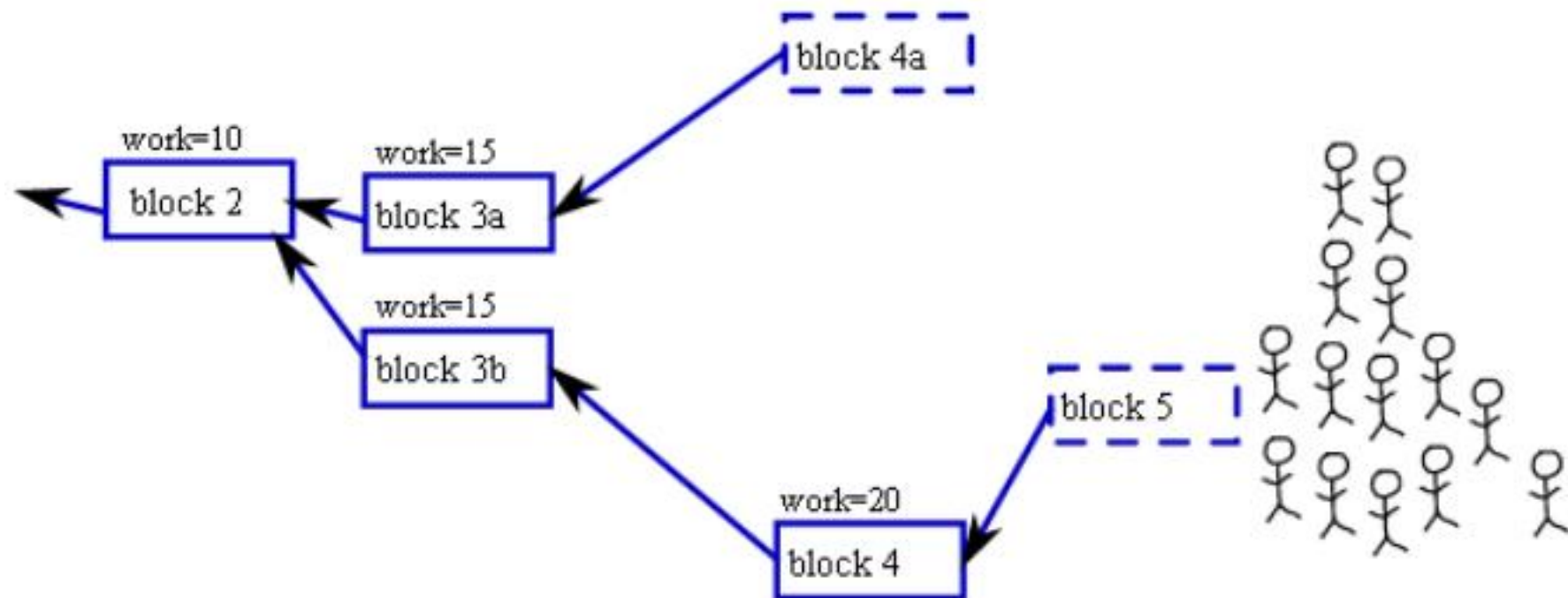
Fork – Miners Mine On Both Branches



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

$(1/100)^2$

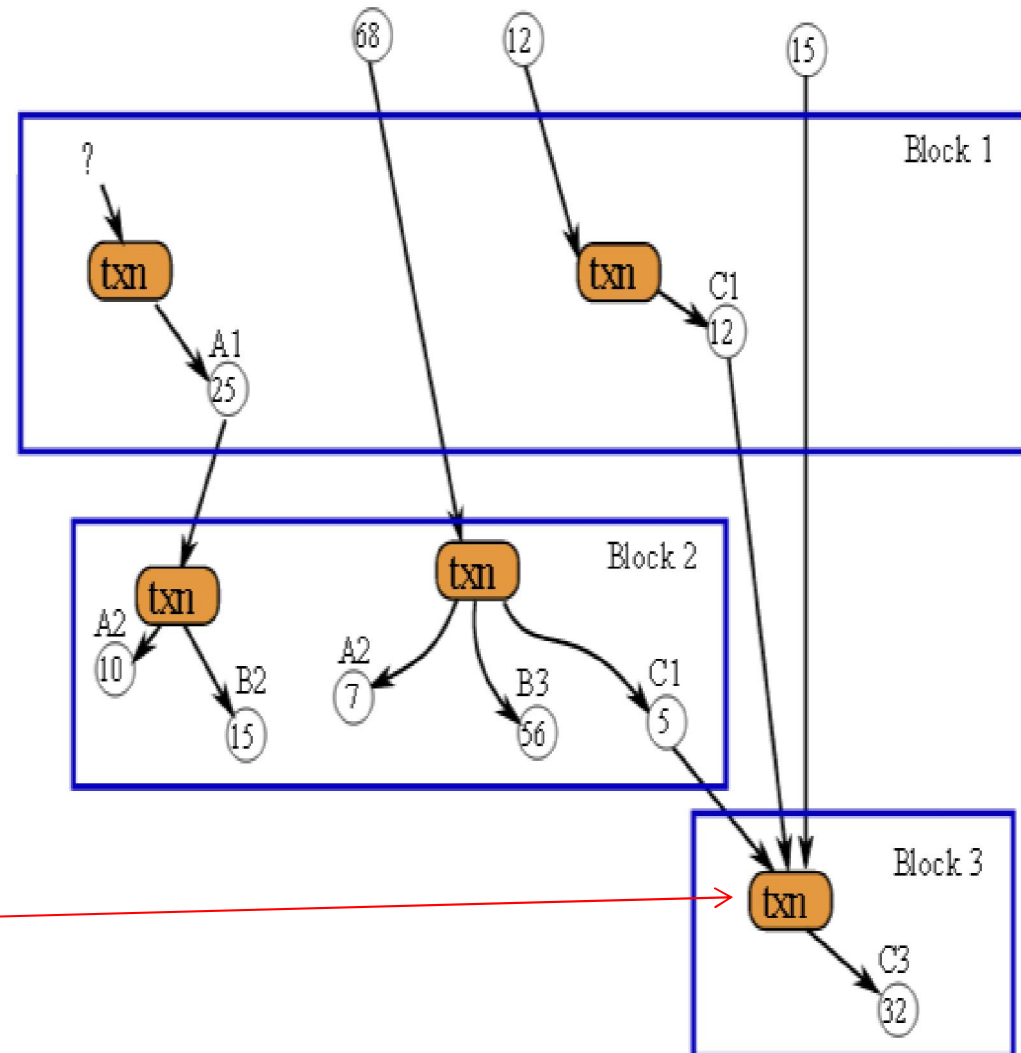
Etc..

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

51% -
Very Famous



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).

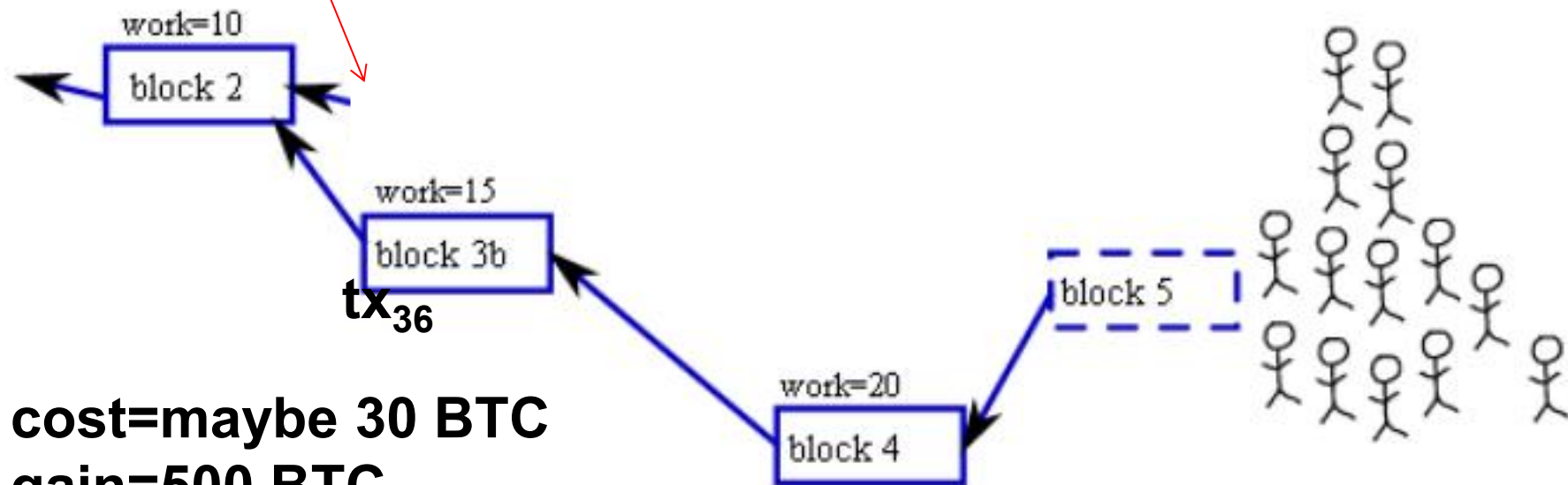
Can be easy or very difficult it depends!



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.

Sirer About 51% - Incredible Claims

“A 51% miner does not have 51% of the vote;
in fact, GHash has just as much say over the contents of the blockchain as
do I, or you, or anyone else”.

"The truth is that it is the Bitcoin users who wield ultimate power, and the
miners' hashing power has absolutely no say
in determining how the protocol evolves"

19 June 2014

<http://hackingdistributed.com/2014/06/19/bitcoin-and-voting-power/>

STRONGLY DISAGREE.

Can anybody in their right mind ever believe what they say?

- usually it is the companies who claim the security problems are inexistent.
and academics will “assume the worst”.

54 • if you cannot even trust the academics anymore, whom can you trust?

Nicolas T. Courtois 2009-2014

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 are EXTREMELY EASY to attack: double-spending is possible.

51% and the Longest Chain Rule



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

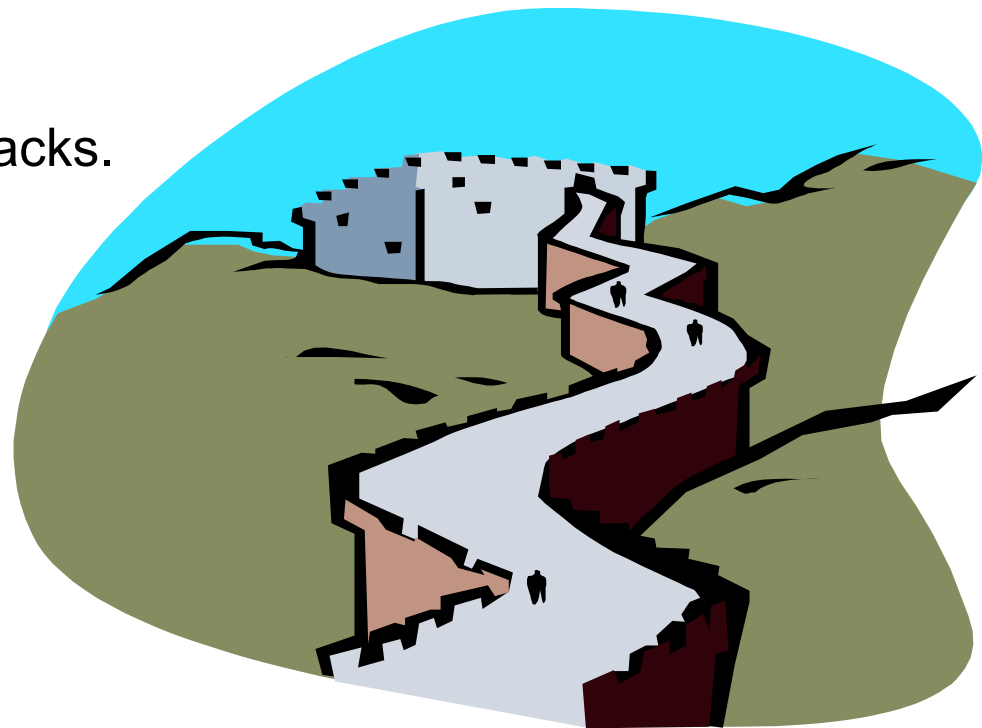
- **Least Common Mechanism** [Saltzer and Schroeder 1975]
 - Poor **Network Neutrality** – miners have excessive discretionary powers...
- => Unnecessary instability and slow transactions...

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, [...]"

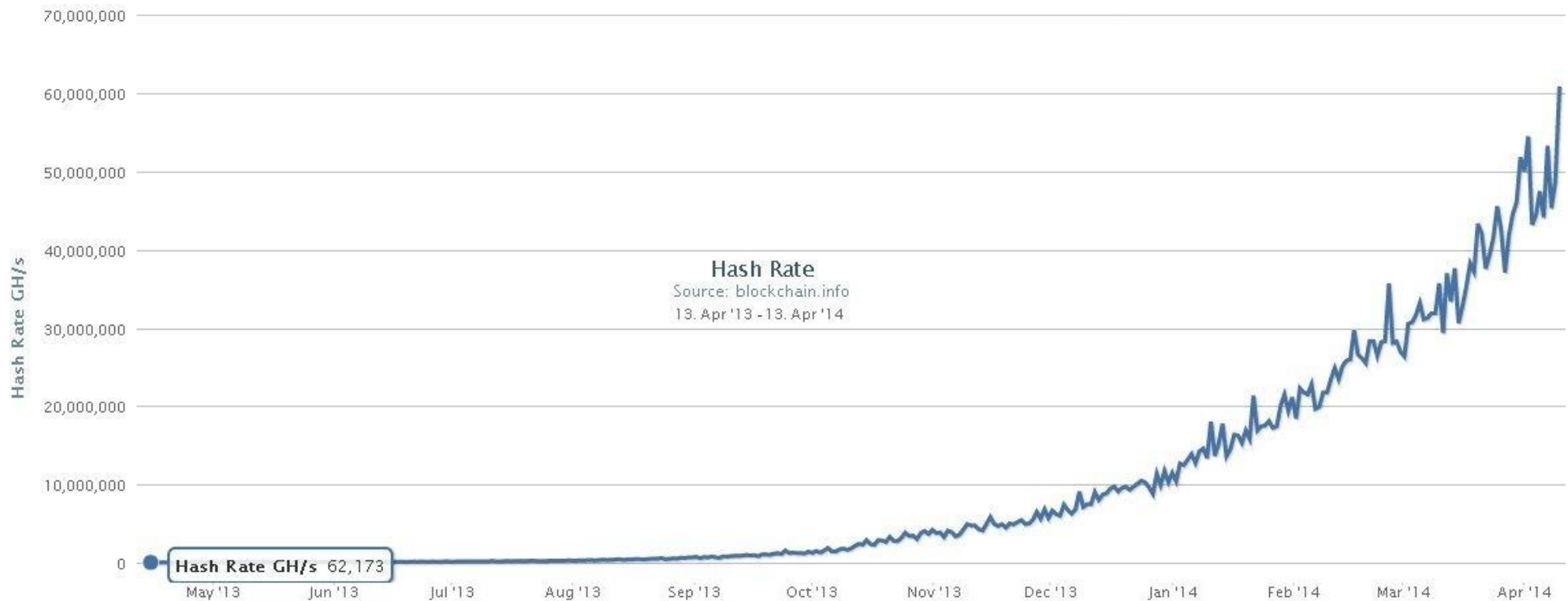
Wow! We have built a "Great Wall".
It protects our money against attacks.

NO THIS IS MISTAKEN



Crazy Hash Power Increase

Nearly doubled every month... 1000x in 1 year.



Thm:

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

60

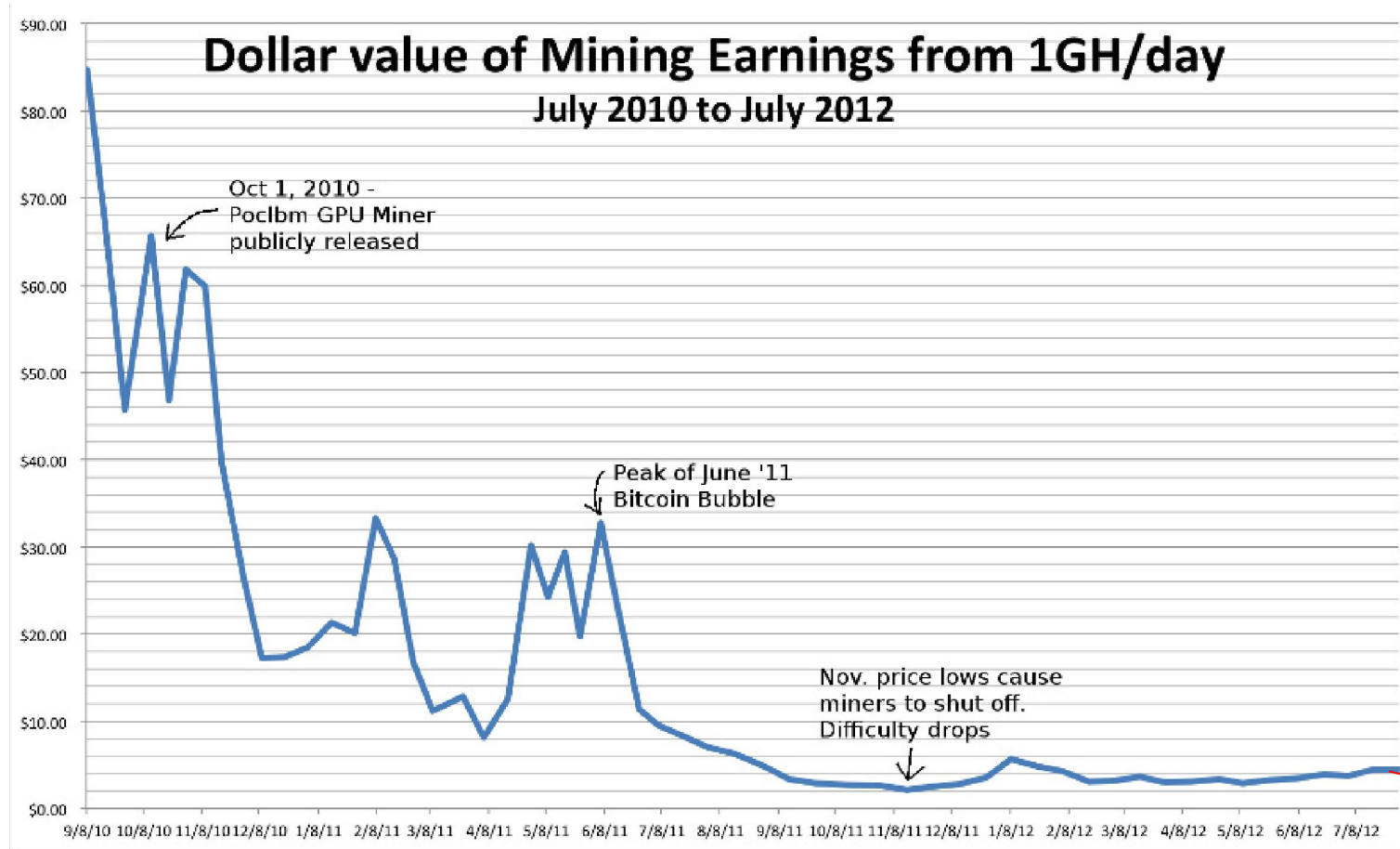
the total income is only **twice** the income for the first month.

In Contrast - Fees

Anybody willing to pay to use bitcoin?



*Revenue Before ASICs



exponential
decrease
after!

Bitcoin Address

To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36
Amount: 1.0 BTC

SEND

Ledger-Based Currency

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

Three formats... (see slides part 3)

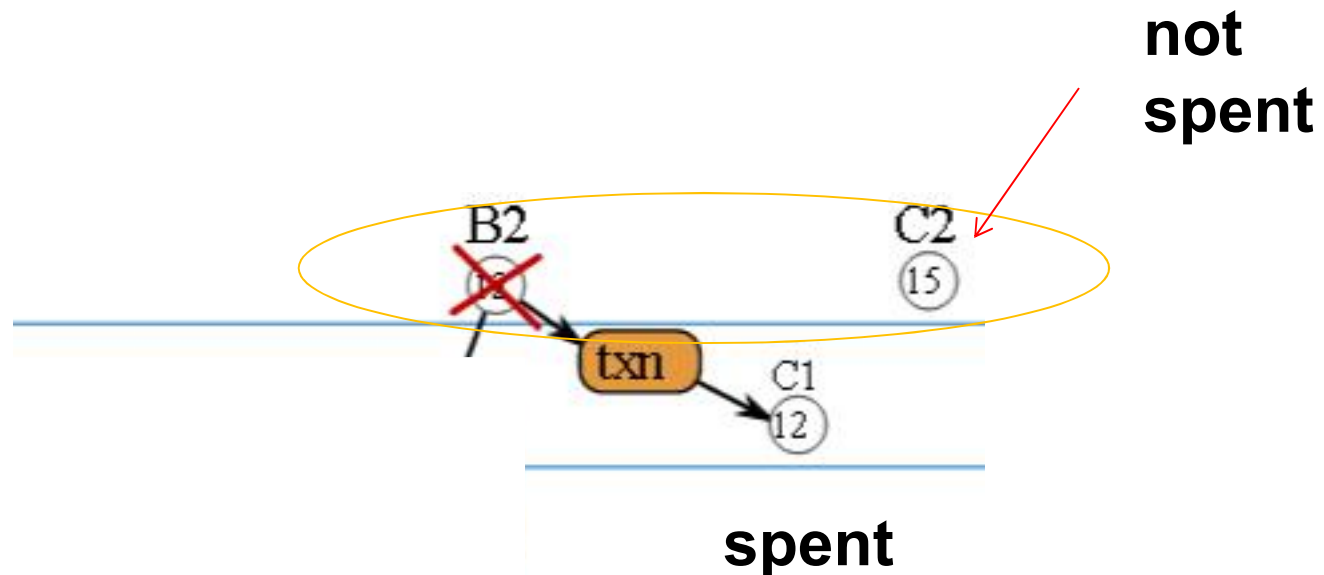
PK itself remains confidential until some part is spent.

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

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).

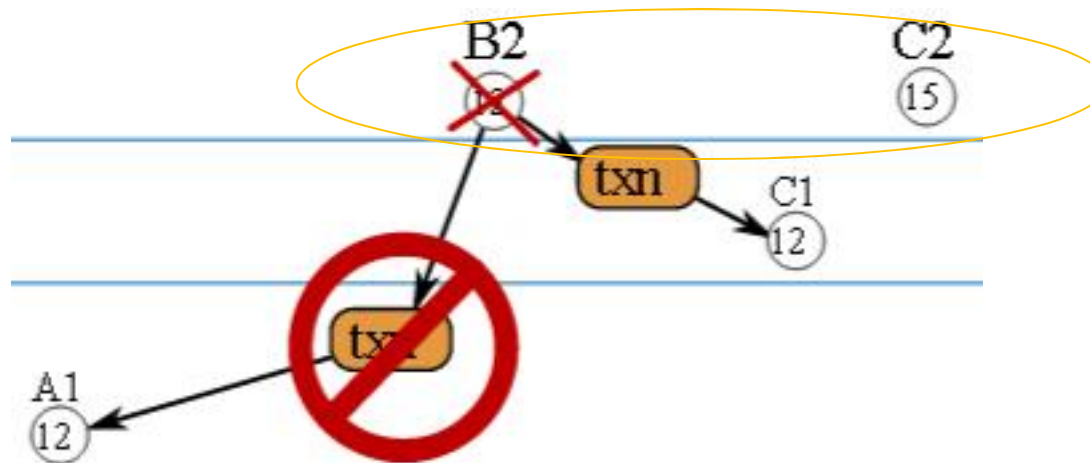


Bitcoin Ownership

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:



Bitcoin Circulation

To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36
Amount: 1.0 BTC

SEND

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)

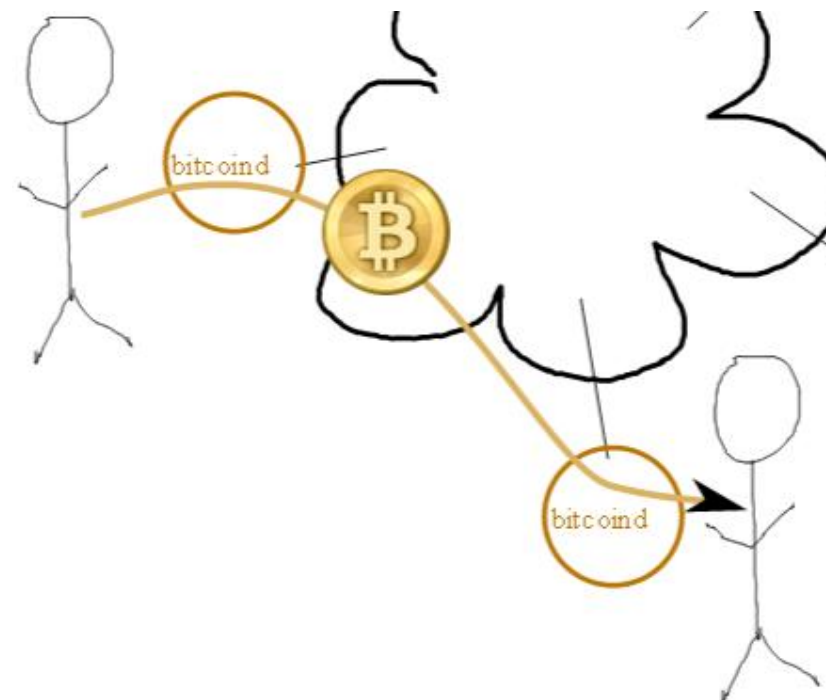
Bitcoin Transactions:

- 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

SEND

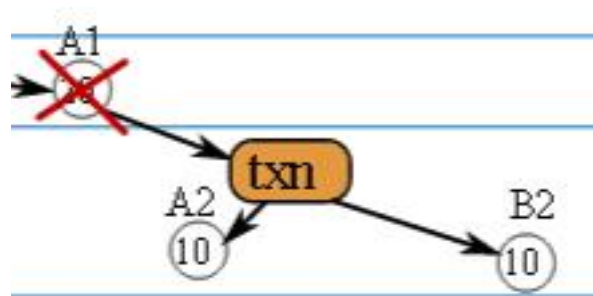


In / Out

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.

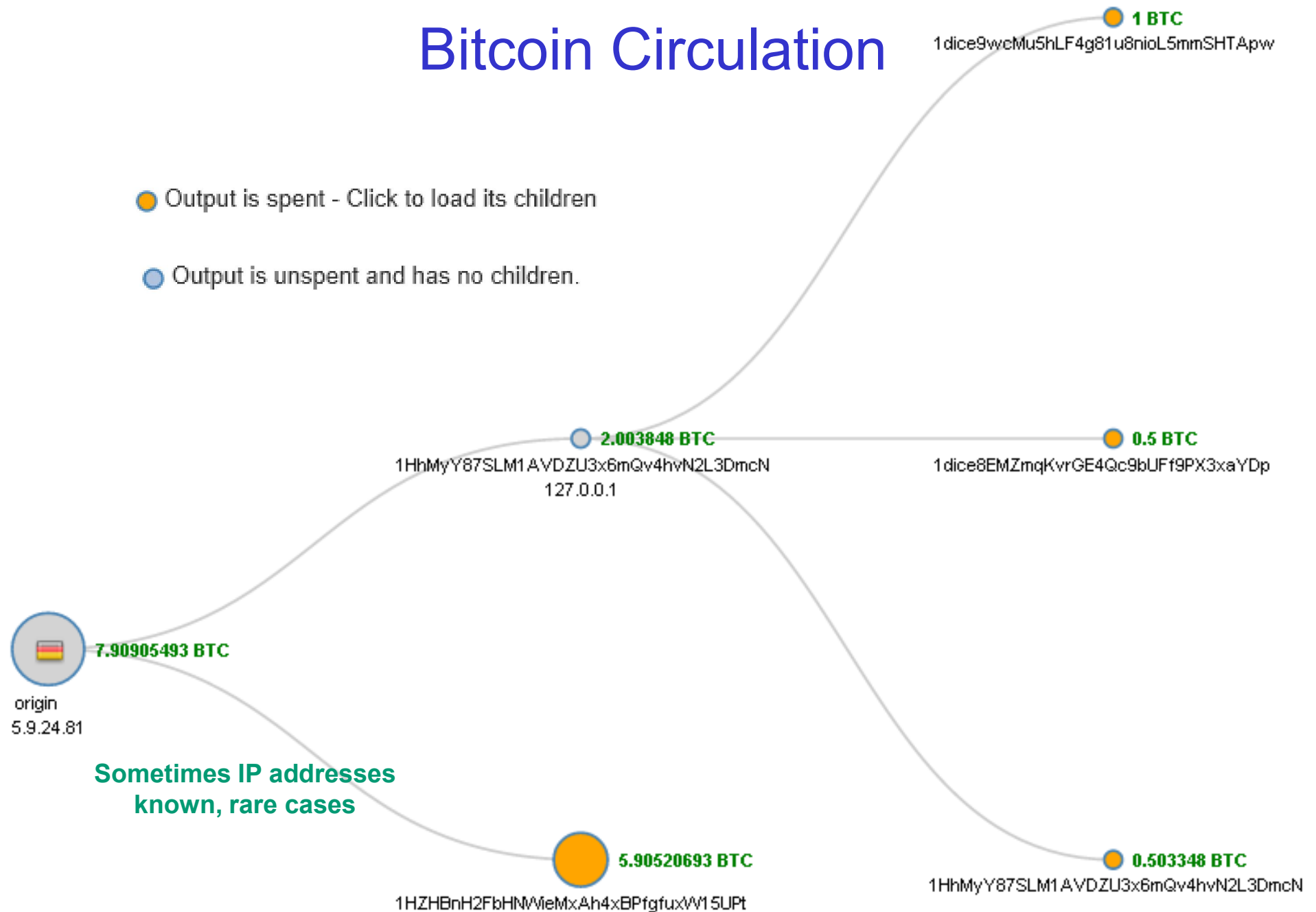


on this picture we
ignore the fees

Bitcoin Transfer

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

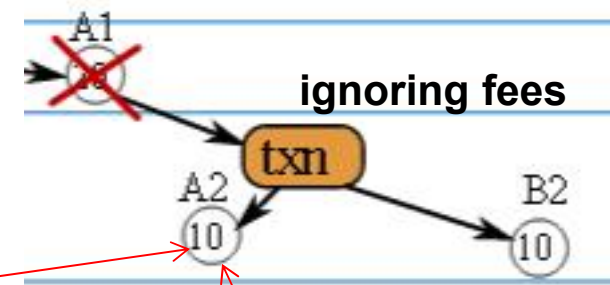
Bitcoin Circulation



Attributions

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)

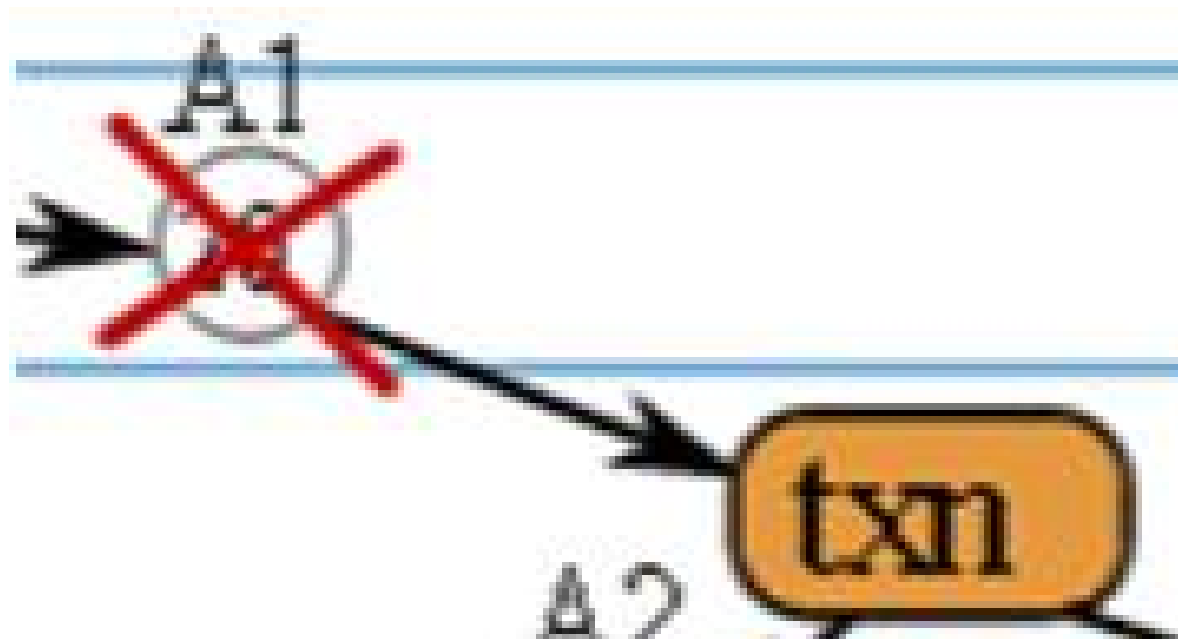


Caveat: Each attribution can be traced back to the initial mining event.

Fragmentation and Summation Rule

Each PK has a balance, say 20 BTC
current balance = $\text{sum}(\text{unspent attributions})$.

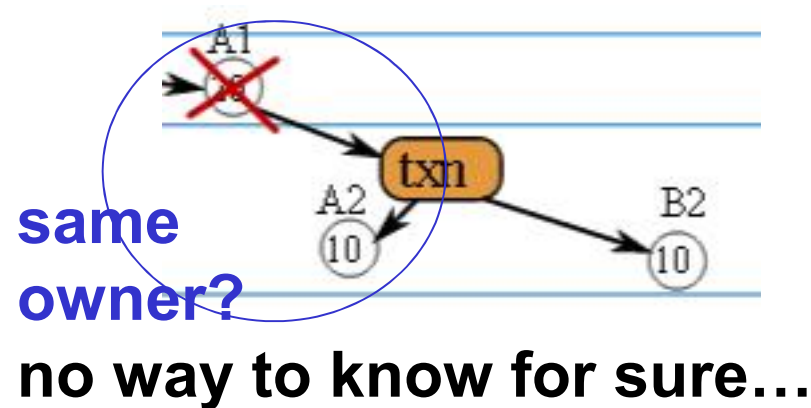
Attributions are ALWAYS destroyed when used,



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...



With Multiple Attributions

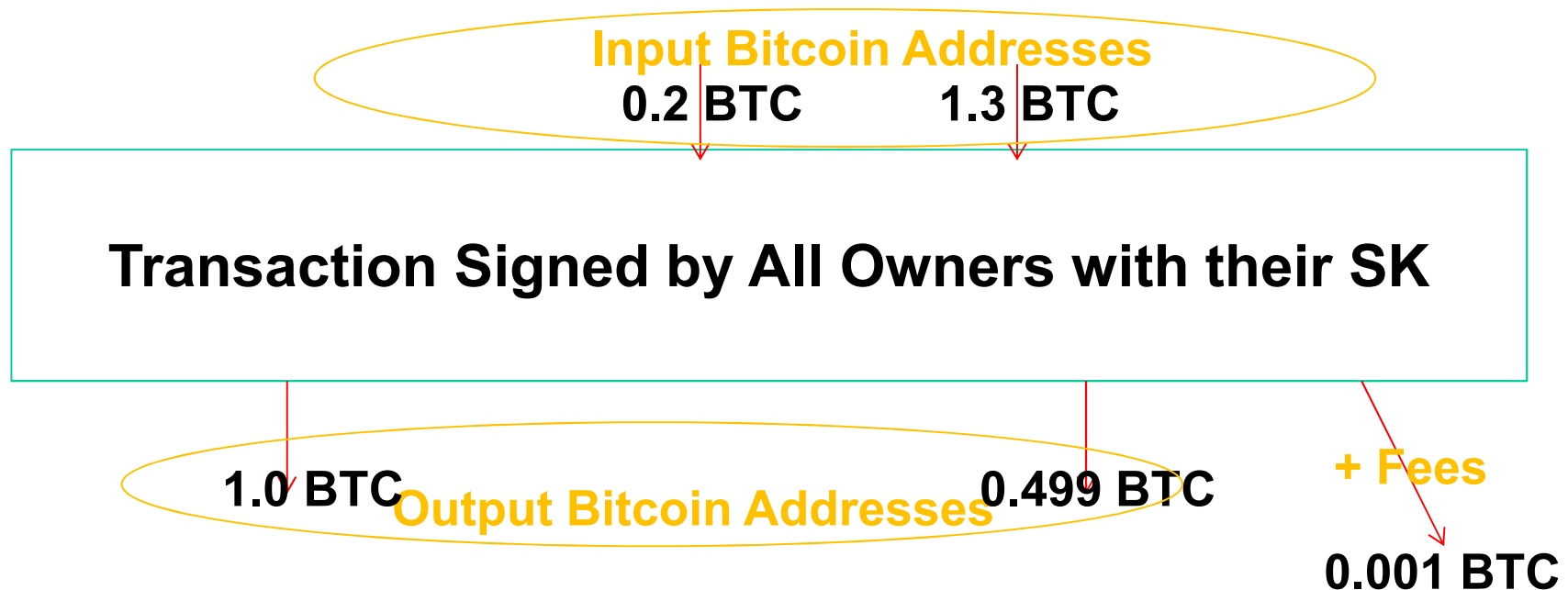


A screenshot of a Bitcoin transaction form. The form has a light green background and a black border. It contains two lines of text: "To: 1K2CcfWYW5sBL2xSeQWxpcmjPCgoXdi36" and "Amount: 1.0 BTC". Below the text is a blue button with the word "SEND" in white capital letters.

typical case, even for a single user

Bitcoin Transfer

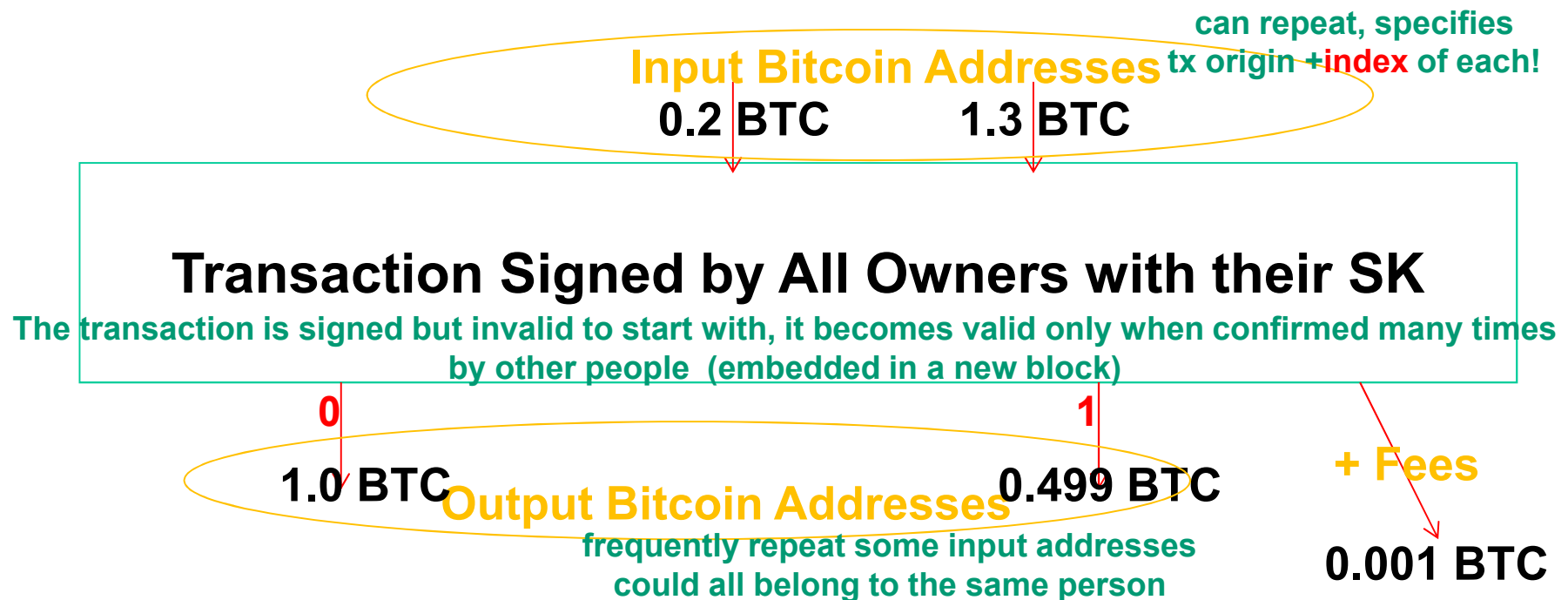
Transactions have multiple inputs and multiple outputs.



Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.

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



Example 1

Transaction View information about a bitcoin transaction

99929d9ad149047ae79998592241ddd7ef4ae2f4bb4e057e9c36c4cefa88830

1EWJJCnBuyQDPwVHuCycUCMHCvXTSGLBvk

1MisJY7KwjnhmdaMwyH6v1A3jDQpty7rdg

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



1BaQzo1SyRXZRhQwSvsQJKAUvi5tu3L9uQ

10 mBTC

1rpU1Wa3pYeuJEbRPMWDDCzeh5PDMBrQ9

83.50001 mBTC

1BSy1ARBQfT9PRDYYB6DvzRkbSVRrgbaX3

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": "ba250a395cf37e2d112859ecd4379a605a6fd8e96b406c4f69901abc05d5b47",
        "n": 1,
      },
      "scriptSig": "304402206dcf0ef7ca4bfa573ed8f3dc94dca42f5ea46827e8885056d3dfede88e52d49b022077055f3d3c125cc"
    }
  ],
  "out": [
    {
      "value": "5.00000000",
      "scriptPubKey": "OP_DUP OP_HASH160 ddc1120deb91acda0d3e5774a2b8908e3424f532 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.

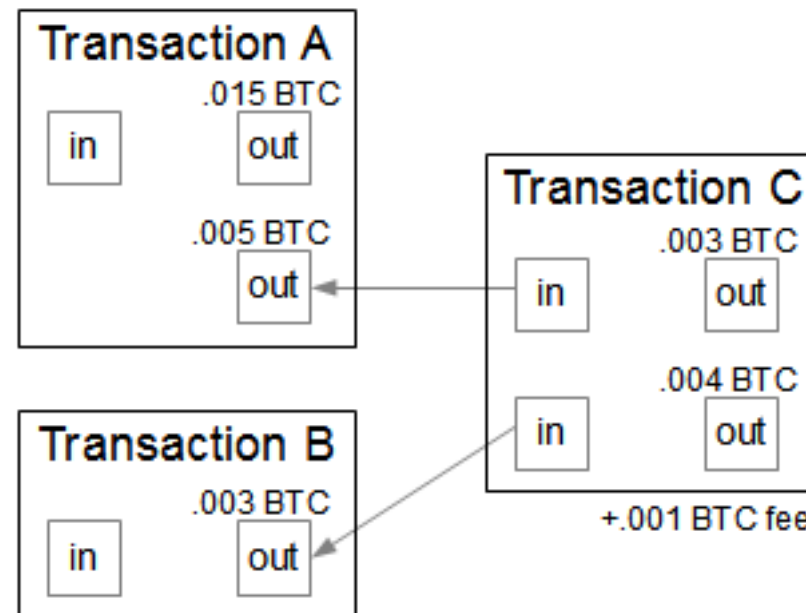
Full bitcoin network nodes stored all transactions ever made and checks their correctness (all the digital signatures).

About 15 Gbytes data, 24 hours full download.

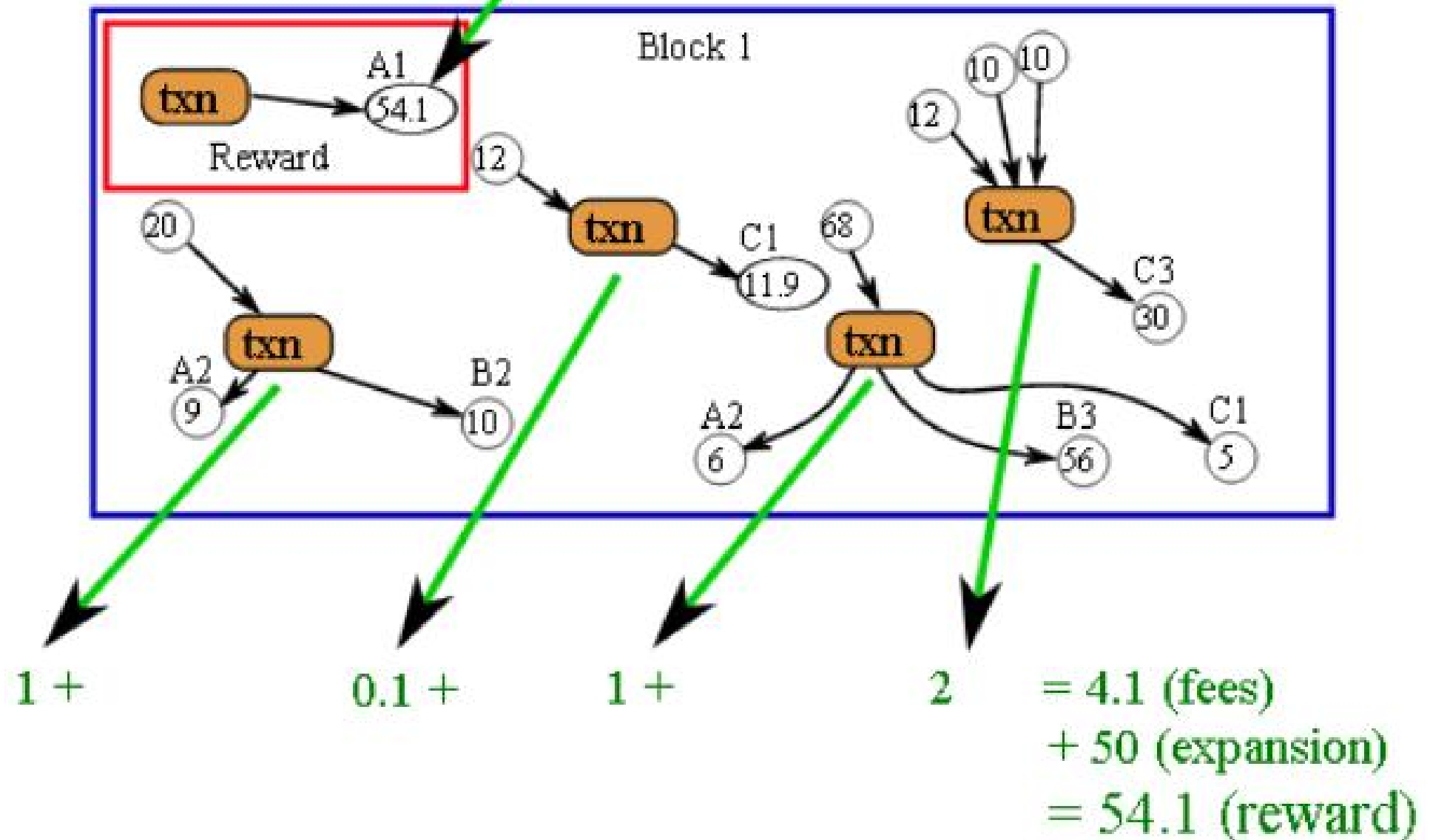
In practice one could skip check for things confirmed by many miners... dangerous though. There is no absolute proof that miners have already checked them (maybe they forgot, a bug).

Transaction Chaining

2 attributions:



Fees => Miner Profit



Bitcoin Mining



BITCOIN MINER

Money Out of Thin Air



Bitcoin vs. Klondike



2012-2014

>100,000 miners

**maybe $\frac{1}{2}$ - $\frac{3}{4}$???? were
victims of scams and
paid for miners which
were not delivered in
reasonable time**



87

BITCOIN MINER†

1896-1899

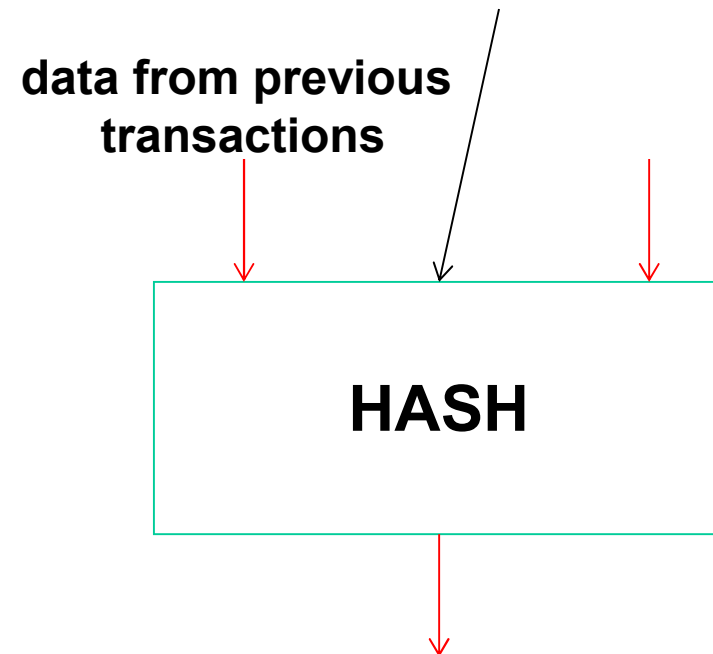
**100,000 miners,
4,000 struck gold**



Bitcoin Mining

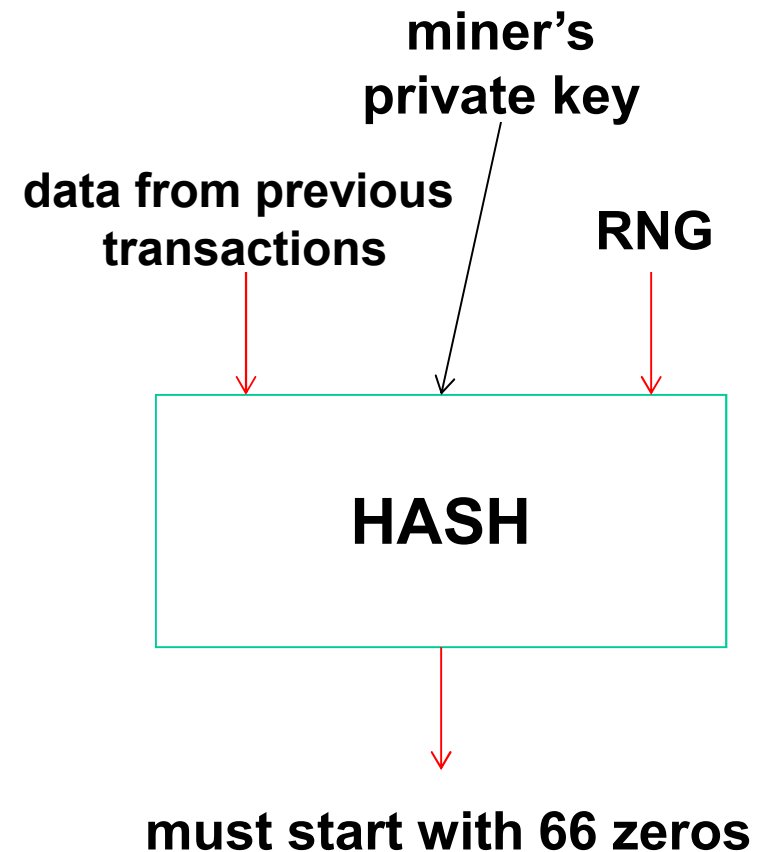
- Minting: creation of new currency.

Creation of “money”
+re-confirmation
of older transactions



*Quiz Question

- What is wrong here?

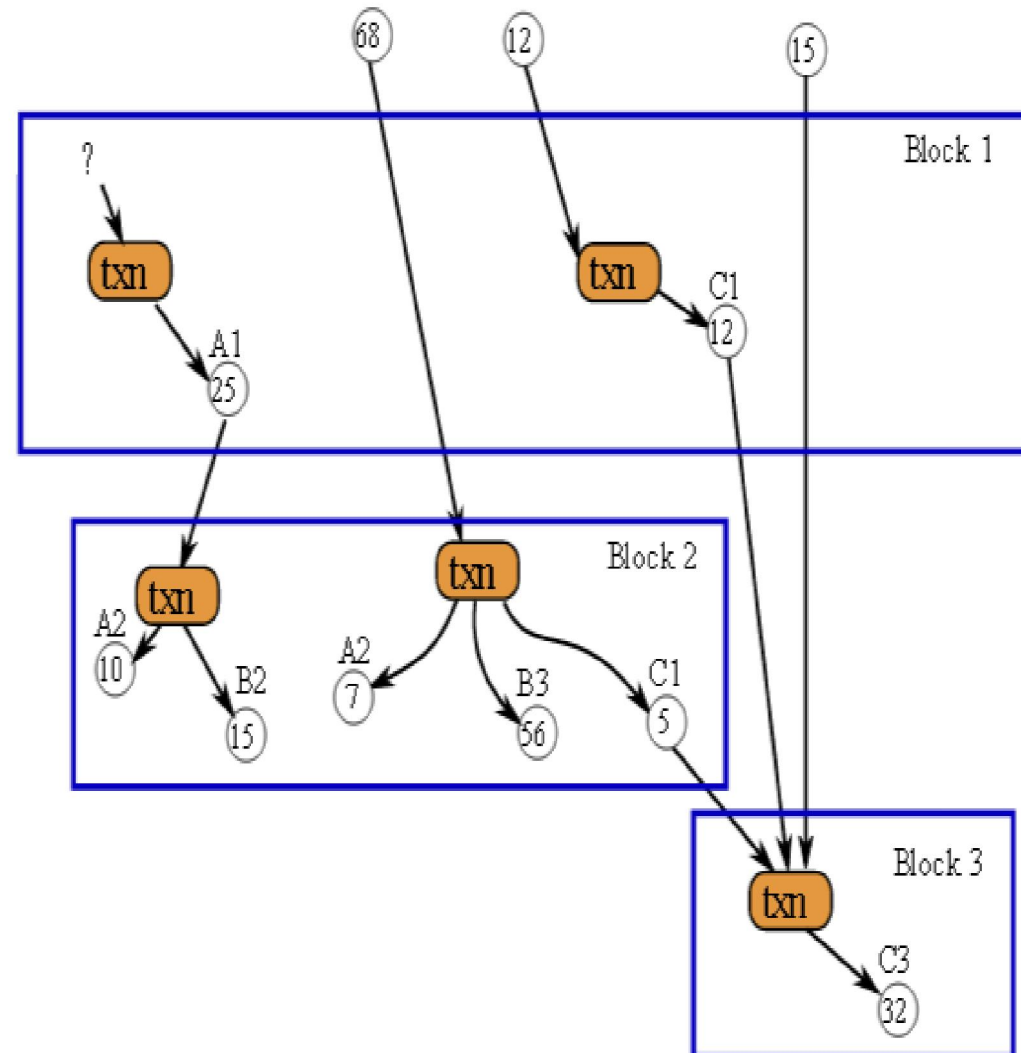


Block Chain

Def:



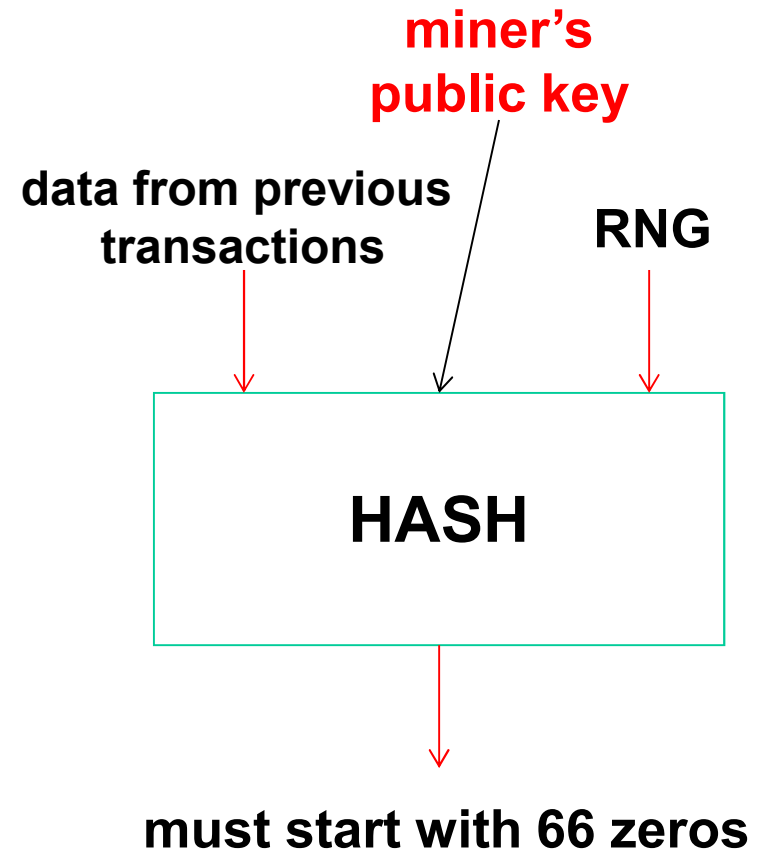
The bitcoin transaction database shared by everyone.



Bitcoin Ownership

Ownership:

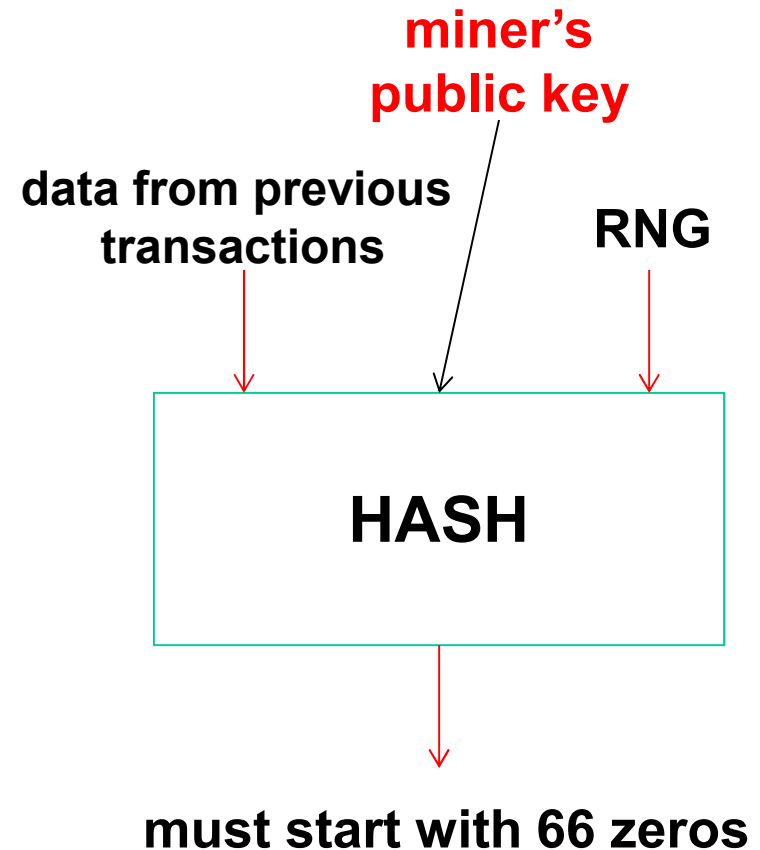
- “policed by miners”:
- only the owner of the can transfer [a part of] 25 BTC produced.



Bitcoin Randomization

Nonce = def?

Which arrow?



Bitcoin Randomization

Nonce = **Number Used Only Once**

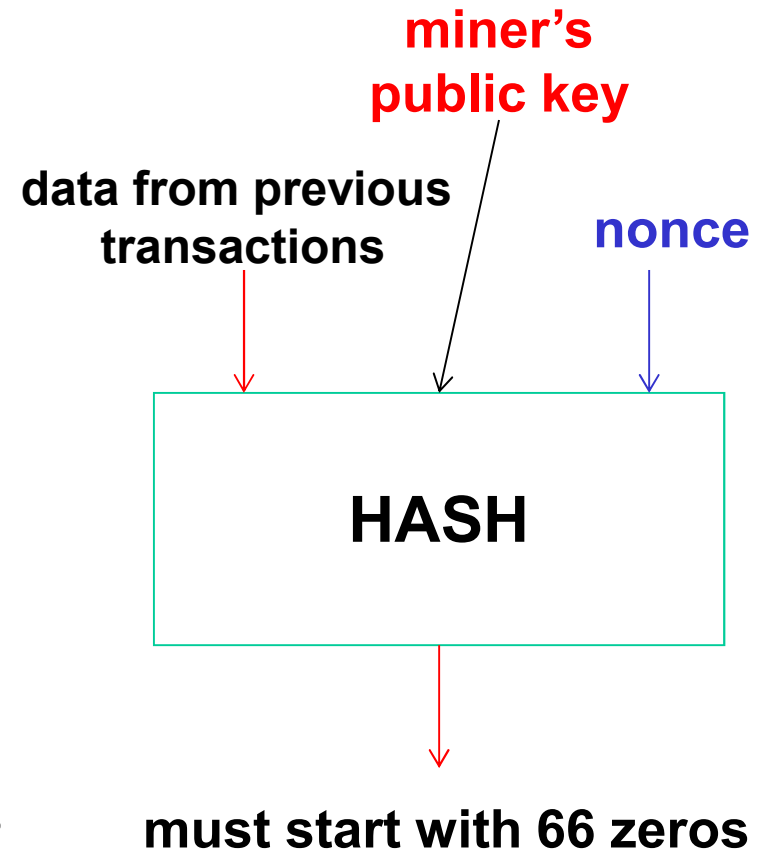
Remark: it does repeat in the main bitcoin block chain [birthday paradox].

Example: 0x04111A63 x 2

What is responsible for that?

What else can be randomized here?

Why this is necessary?

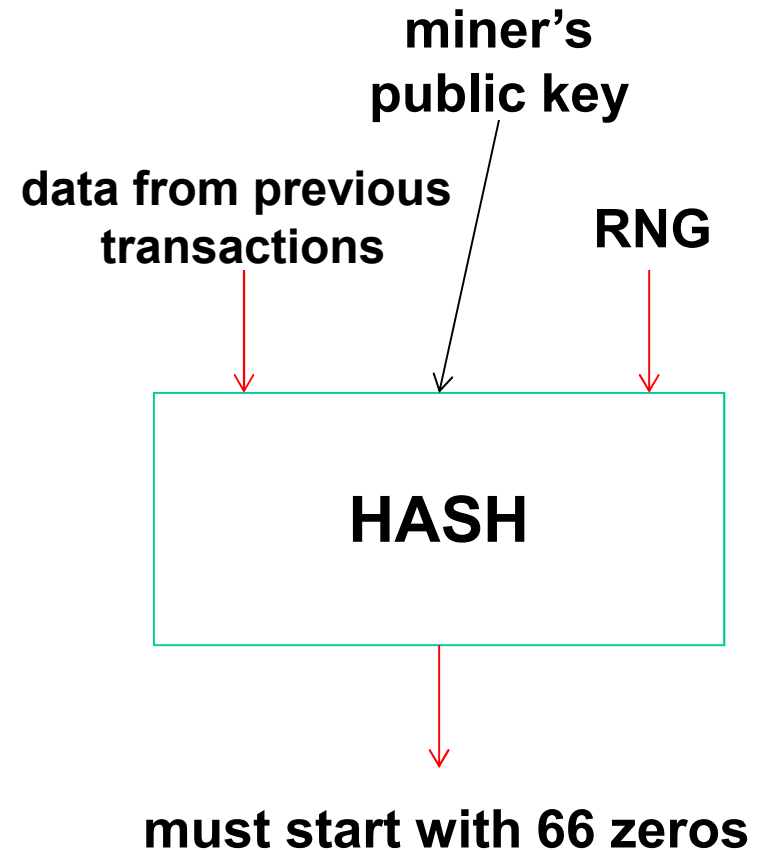


Bitcoin Mining

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

Random Oracle – like mechanism.

What????????????????



Bitcoin Mining

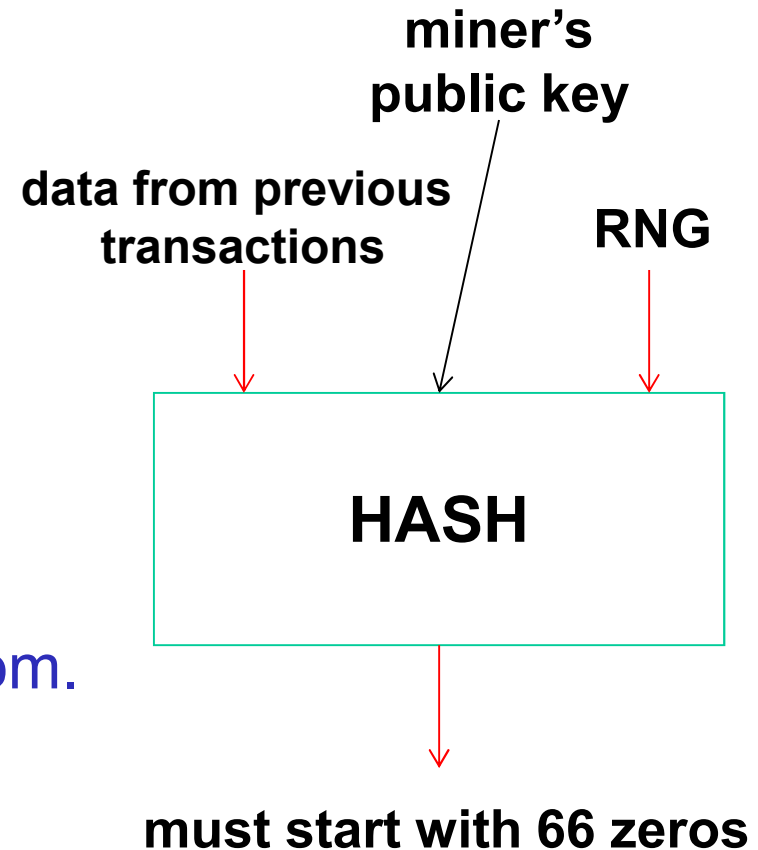
- Minting: creation of new currency.
Creation+re-confirmation
of older transactions

Random Oracle – like mechanism

Means: treat as a DETERMINISTIC
black box which answers at random.

YES it is...

However now I'm going to show it isn't.



Bitcoin Mining

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

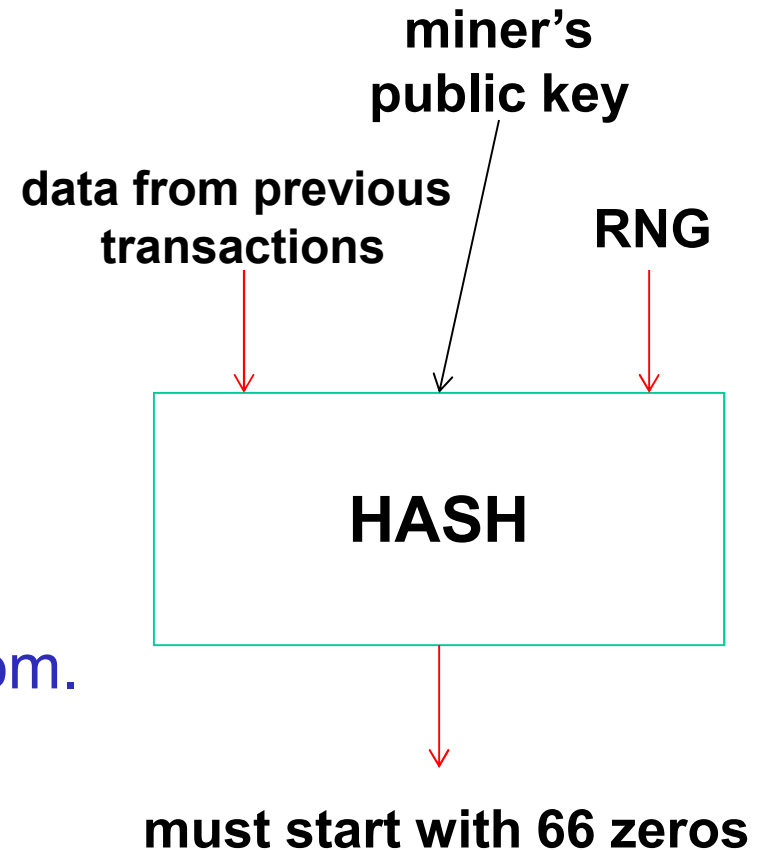
Random Oracle – like mechanism

Means: treat as a DETERMINISTIC
black box which answers at random.

YES it is,

However now I'm going to show it isn't.

Marginal improvement (a constant factor).



Five Generations of Miners

1. CPU Mining

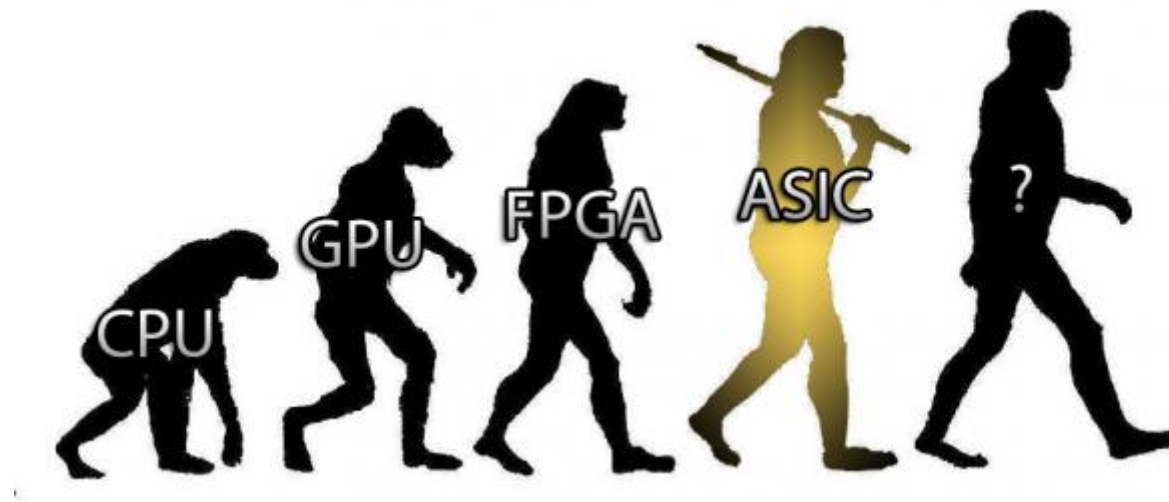
Example:

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

CPU = about 4000 W / Gh/s



Four Generations



Four Generations of Miners

2. GPU Mining

Example:

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

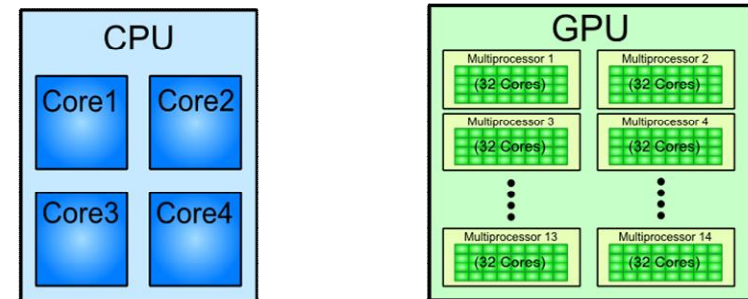
CPU = about 4000 W / Gh/s, in this case

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, in this case

Four Generations of Miners

3. FPGA Mining

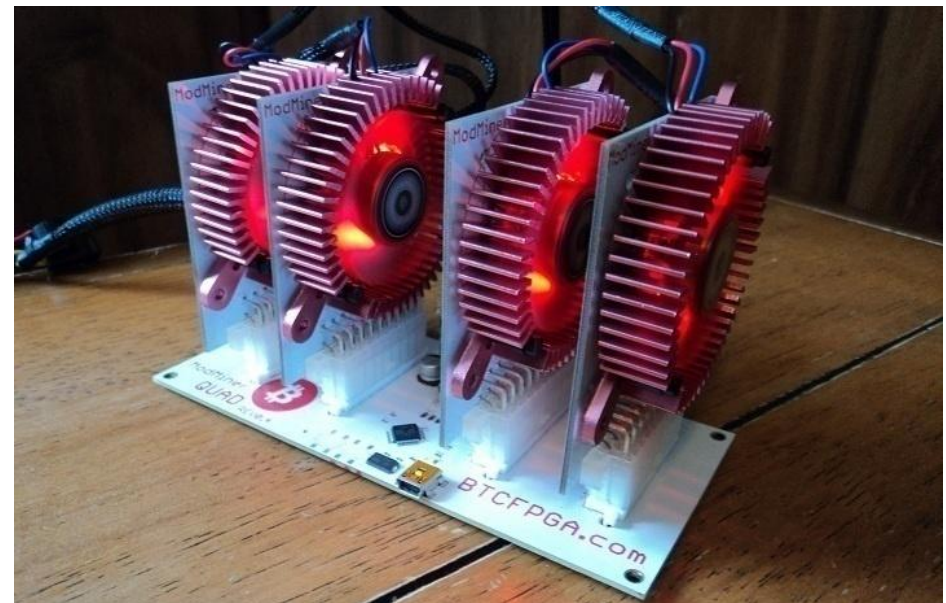
Example:

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

FPGA: 100x less energy.

Still much less with ASIC:

Good points: asynchronous logic, arbitrary gates, etc..

Drawback: hard to update!

Another 10 – 100 times improvement.

(100x is cheating:

I was comparing one 28 nm ASIC
to one 45 nm FPGA)

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...

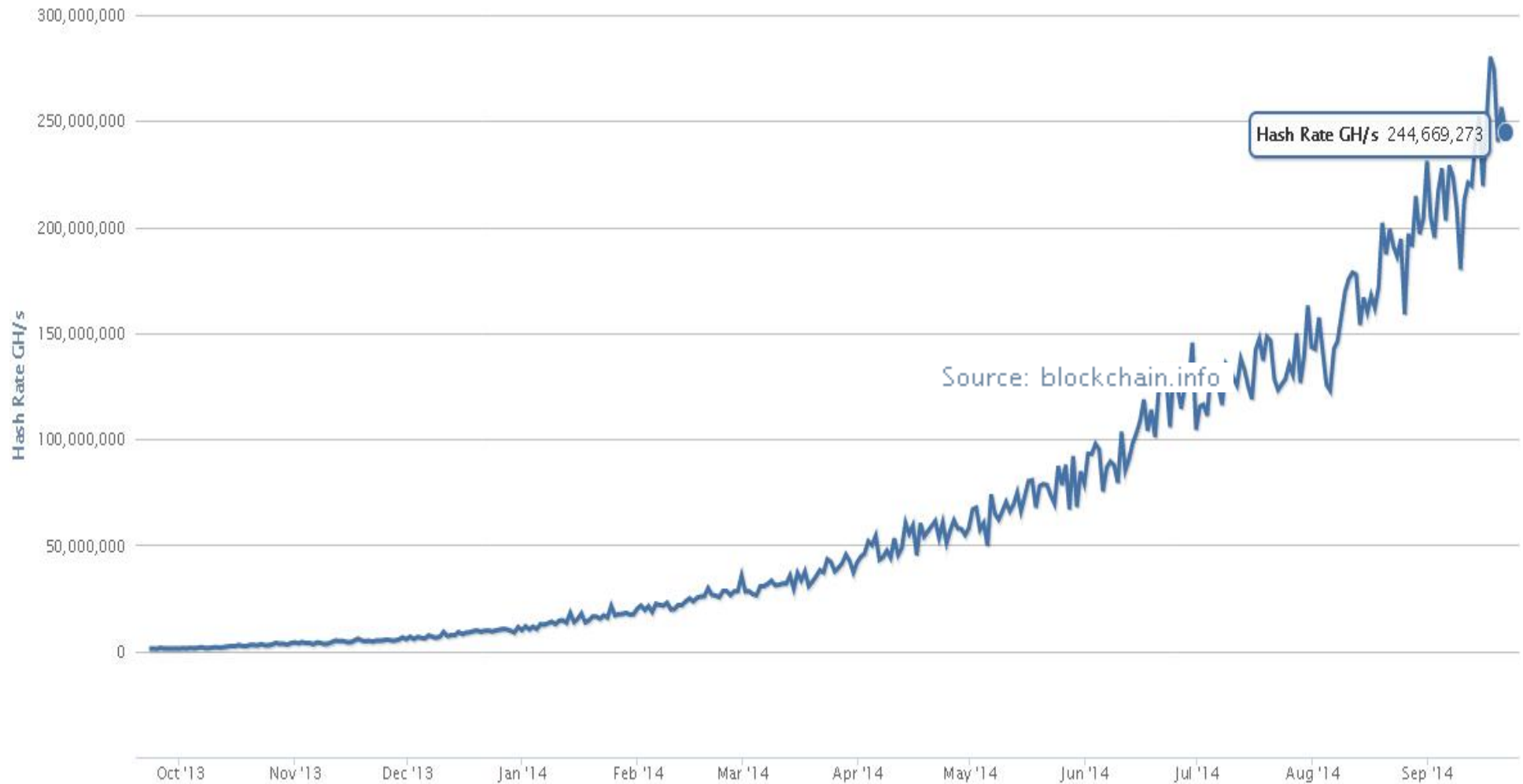
Like 1000% per year improvement.

Hash Rate - Doubled Nearly Every Month!

1000x in 1Y



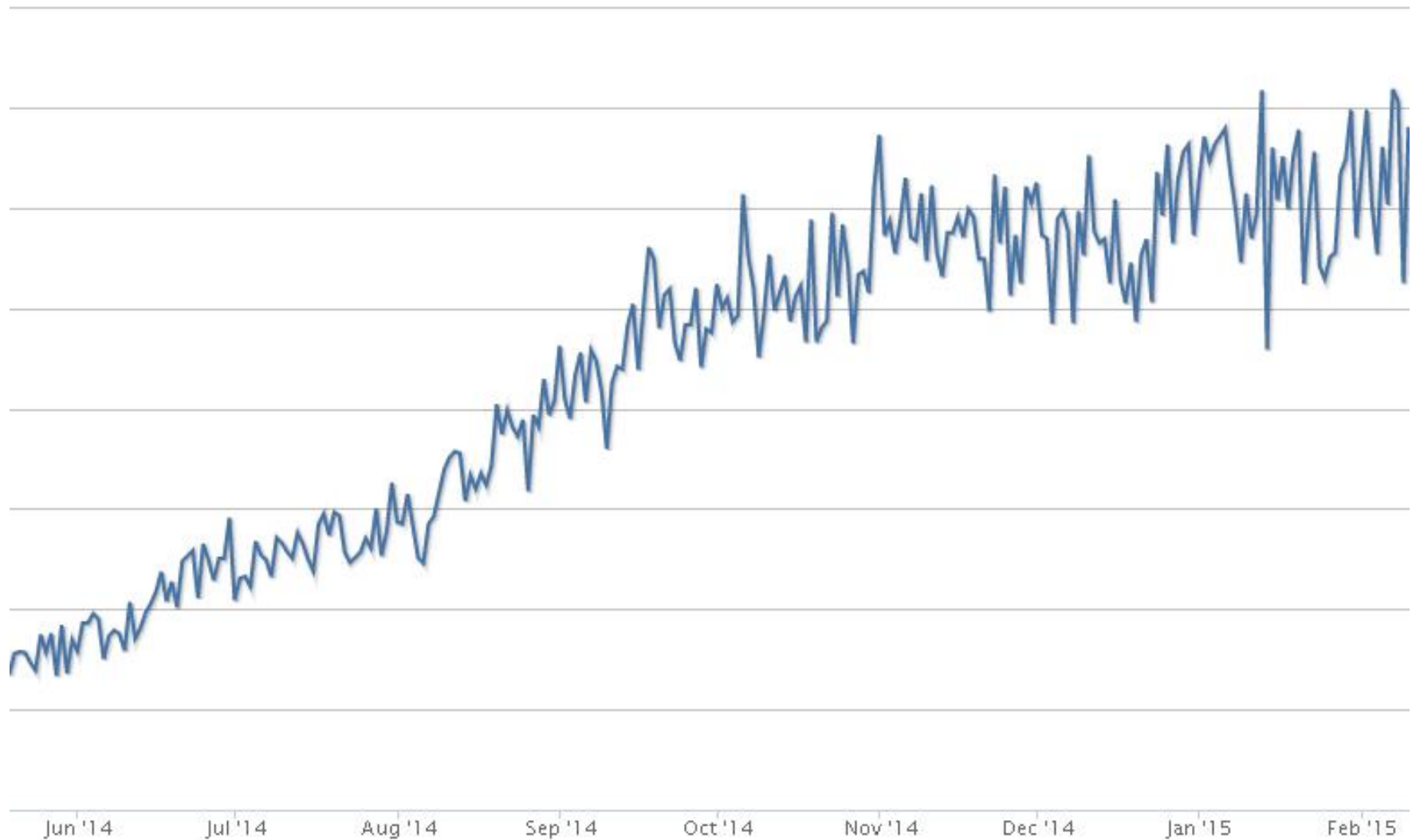
Sep 2014: +60% Every Month



Jan 2015: Peak Reached

Hash Rate

Source: blockchain.info



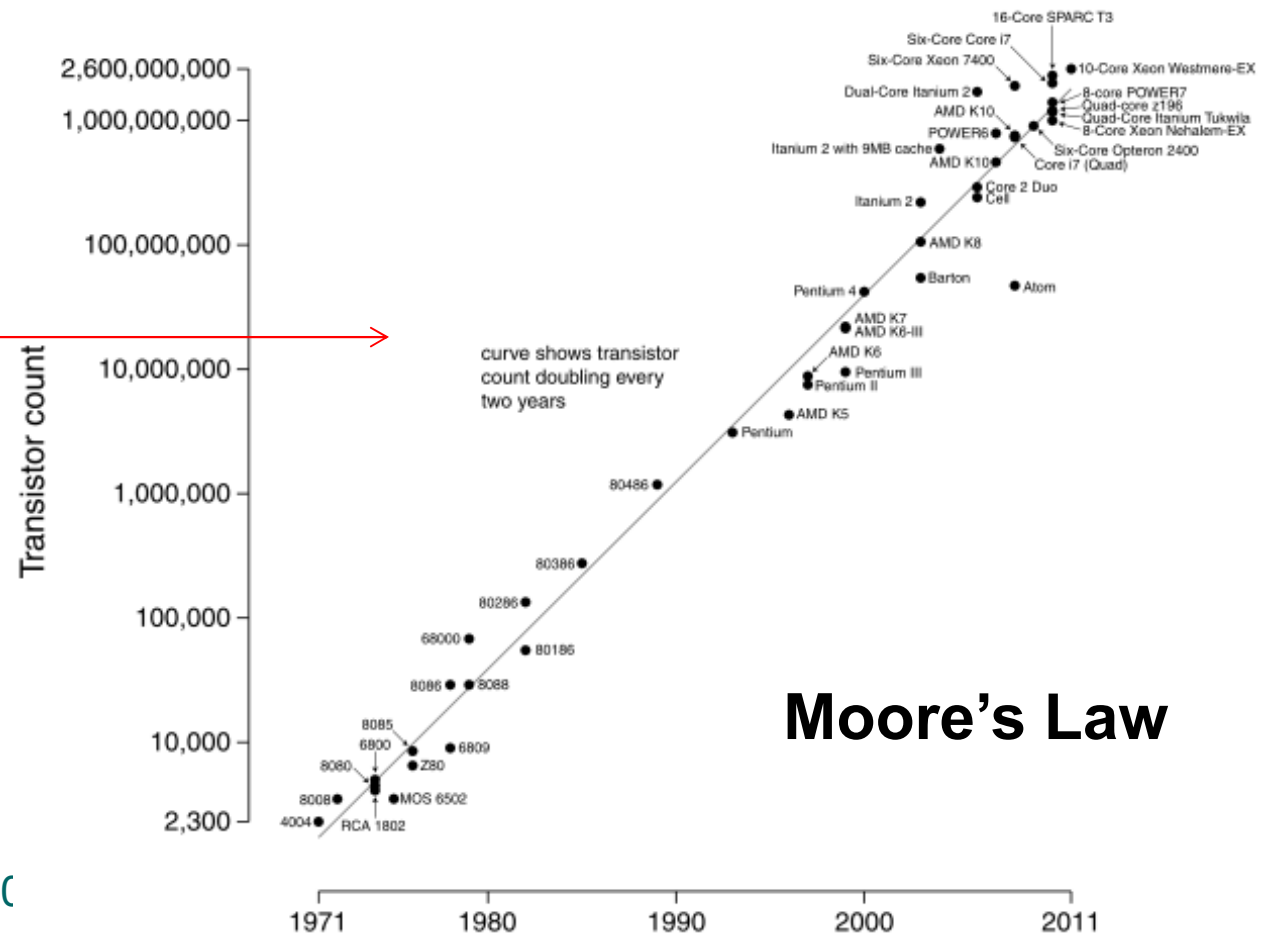
Five Generations of Miners!

5. Quantum Miners?

Business Law:

Every technology
improved by
30%, 67%,
each year?

why not 1000% ???



Butterfly Labs

and their
angry customers



BUTTERFLYLABS

What's New? | Articles | Forum | Blogs | FAQ | Classifieds

New Posts | FAQ | Calendar | Community ▾ | Forum Actions ▾ | Quick Links ▾

Forum ▸ Butterfly Labs ▸ Post Sales & Customer Service ▸ I am angry because.....

Thread: I am angry because.....

LinkBack ▾ | Thread Tools ▾ | Search Thread ▾ | Display ▾ | 10-22-2013, 01:08 PM #1

my 3rd minirig order from 31 Oct 2012 hasn't shipped yet either!

I am not getting a reply to my email
By BFL_Josh in forum Frequently Asked
Replies: 2
Last Post: 02-22-2013, 01:51 PM

Refund because of (again!) delayed shipping?
By Frizz23 in forum Pre-Sales Questions
Replies: 14
Last Post: 10-25-2012, 02:34 PM

Promised 1 W per GH/s, delivered 3.2 W to customers



BFL power consumption / Charity Donation

March 29, 2013, 07:40:01 AM

We are so confident in our power consumption

If our power targets end up consuming more than 1.1w of power per gigahash, we will donate 1000 BTC to charity! How is that for confidence in our power usage?



Better Miners: less nm

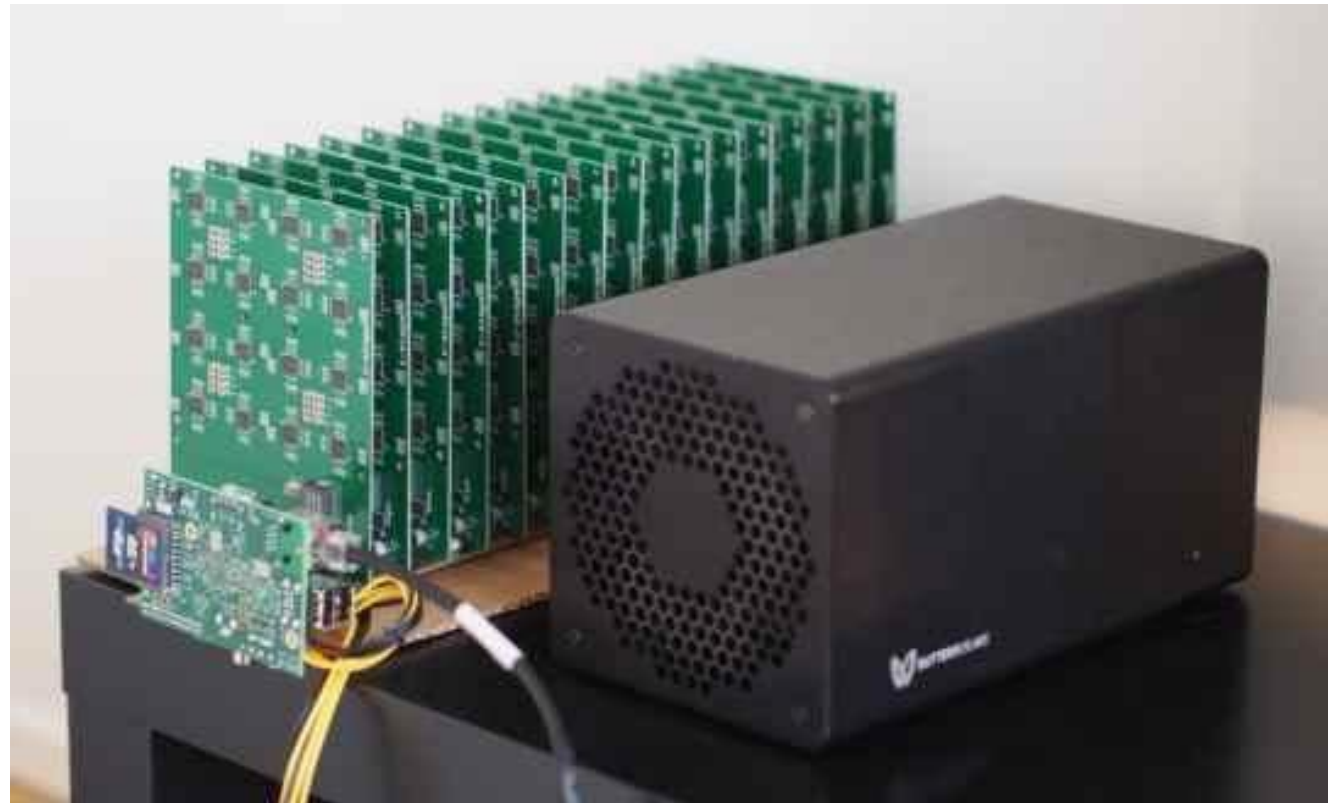
KNC

vs.

BitFury

vs.

Butterfly

109 **20 nm****28 nm****65 nm**

ASICs Comparison

By power / Gh/s



0.35 W low power mode



1 W



cf. https://en.bitcoin.it/wiki/Mining_hardware_comparison



Criminal Scams

See bitcoinscammers.com

os://www.hashblaster.com

✉ info@hashblaster.com 📍 Thea-Leymann-Straße 47, Essen, Germany



HOME

TECH SPECS

FAQ

ABOUT US

CONTACT US

PRE-ORI

THE HASHBLASTER "I"

The first 20nm bitcoin miner
Join the mining revolution !

Pre-order yours for just \$8,799 - Shipping Q1. 2014

Immoral Business Practice

I do not know a single company which is totally honest.

By consumers, for consumers...

Ripoff Report®

KNC and Cointerra has been the most honest IMHO,
but worked mostly with pre-orders.

=> huge problem

Class Action Lawsuit: CoinTerra Seeks Out-of-Court Settlement



Austin Hill

@austinhill

+ Follow

I'm preparing a class action lawsuit against @kncminer for failure to refund, non-response & I'm alleging fraud. Anyone want to be included?



Miners for Cash

Available since April 2014.

Quickly falling prices.



Before:

it was IMPOSSIBLE for miners to evaluate the profitability of their investments.

Waiting for 6 months is like getting.... 50 TIMES smaller return, like 2% of the original expected income for a miner...

New Miners

Cointerra Q1 2015:

4.5 TH/s, 1300 W, 2500 USD, 16nm, 14 M\$ investment?

$\Rightarrow 0.225$ W per Gh/s

Total Cost? About 2.0 Billion USD

Quick estimation of the cost of hardware as of April 2014:

Current hash rate 40,000 Th/s (April 2014)

Assume most people use Neptune first generation which costed 3500 USD for 0.25 Th/s of hash power (better devices exist frankly just in pre-orders, well for a majority of people).

So current hash rate might have costed $40,000 \times 4 \times 3,500$ USD, so maybe 600 M dollars in hash equipment.

However probably most people still use miners NOT as good as Neptune, then probably this is 2 times more... So maybe it is already more than 1 billion today.

$600 \text{ M} / 100 \text{ K people} = 6000 \text{ USD typical investment?}$

Bitcoin And Hash Functions



Digest

Our Paper:

arxiv.org/abs/1310.7935

The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining

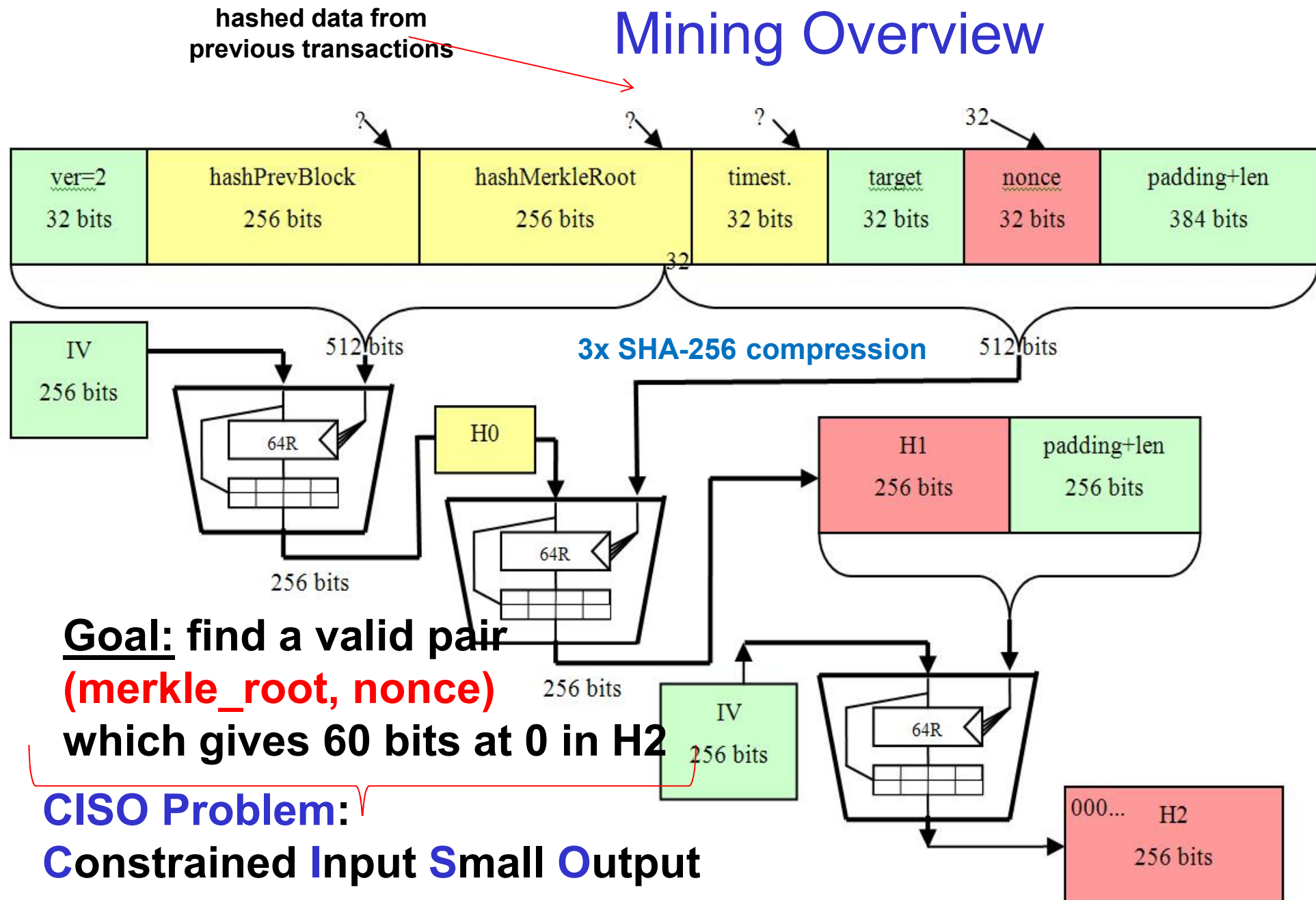
Nicolas T. Courtois¹, Marek Grajek² and Rahul Naik¹

¹ University College London, UK, ² Independent researcher and writer, Poland

Abstract. Bitcoin is a “crypto currency”, a decentralized electronic payment scheme based on cryptography. It implements a particular type of peer-to-peer financial anarchy. It has very recently gained excessive popularity and attracted a lot of attention in the mainstream press and media. Scientific research on this topic is less abundant. A paper at Financial Cryptography 2012 conference explains that Bitcoin is a system which *uses no fancy cryptography, and is by no means perfect* [4].

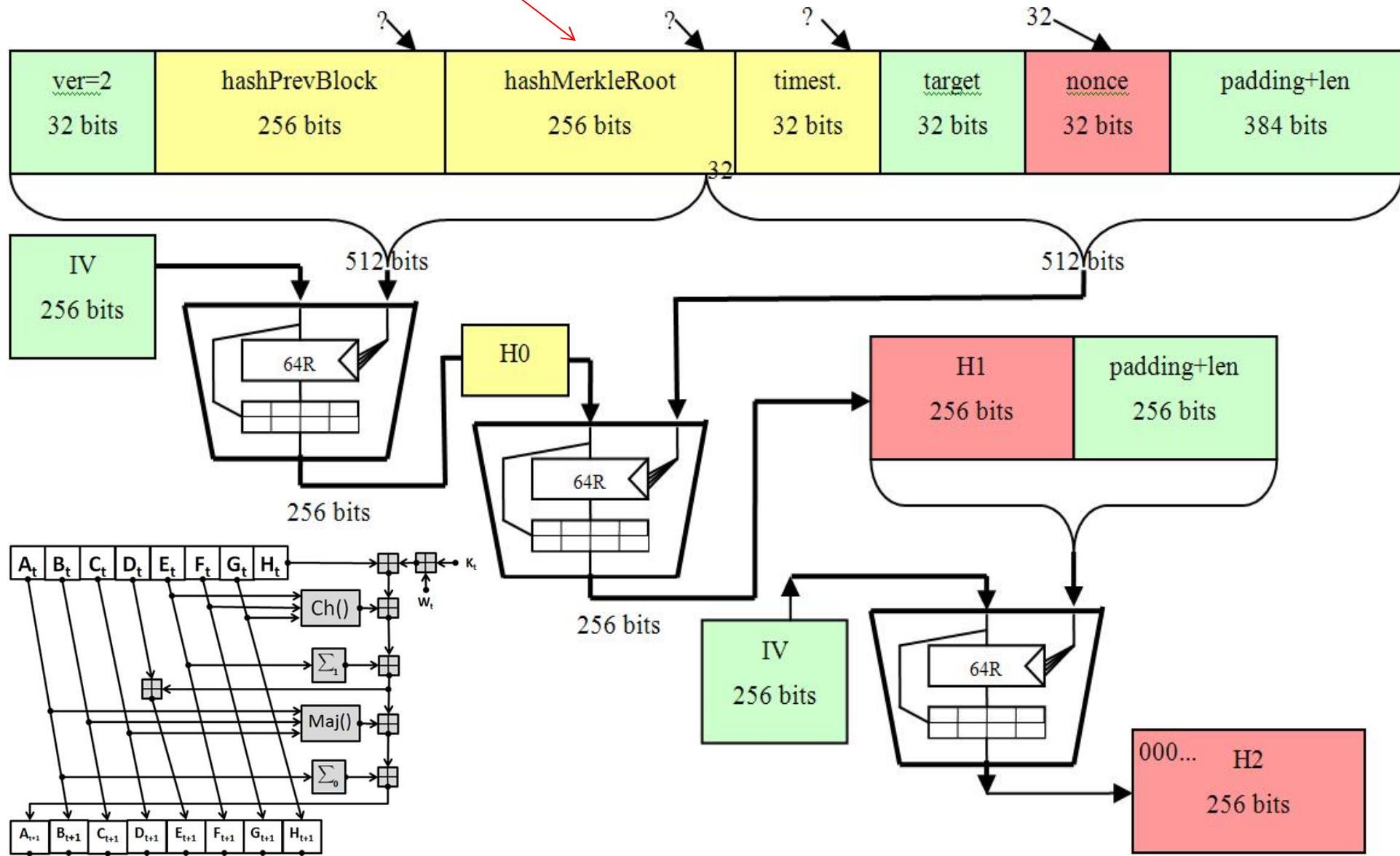
Bitcoin depends on well-known cryptographic standards such as SHA-256. In this paper we revisit the cryptographic process which allows one to make money by producing new bitcoins. We reformulate this problem as a specific sort of Constrained Input Small Output (CISO) hashing problem and reduce the problem to a pure block cipher problem, cf. Fig. 2. We estimate the speed of this process and we show that the amortized cost of this process is less than it seems and it depends on a certain cryptographic constant which is estimated to be at most 1.86. These optimizations enable bitcoin miners to save tens of millions of dollars per year in electricity bills.

Mining Overview



hashed data from
previous transactions

Mining Internals

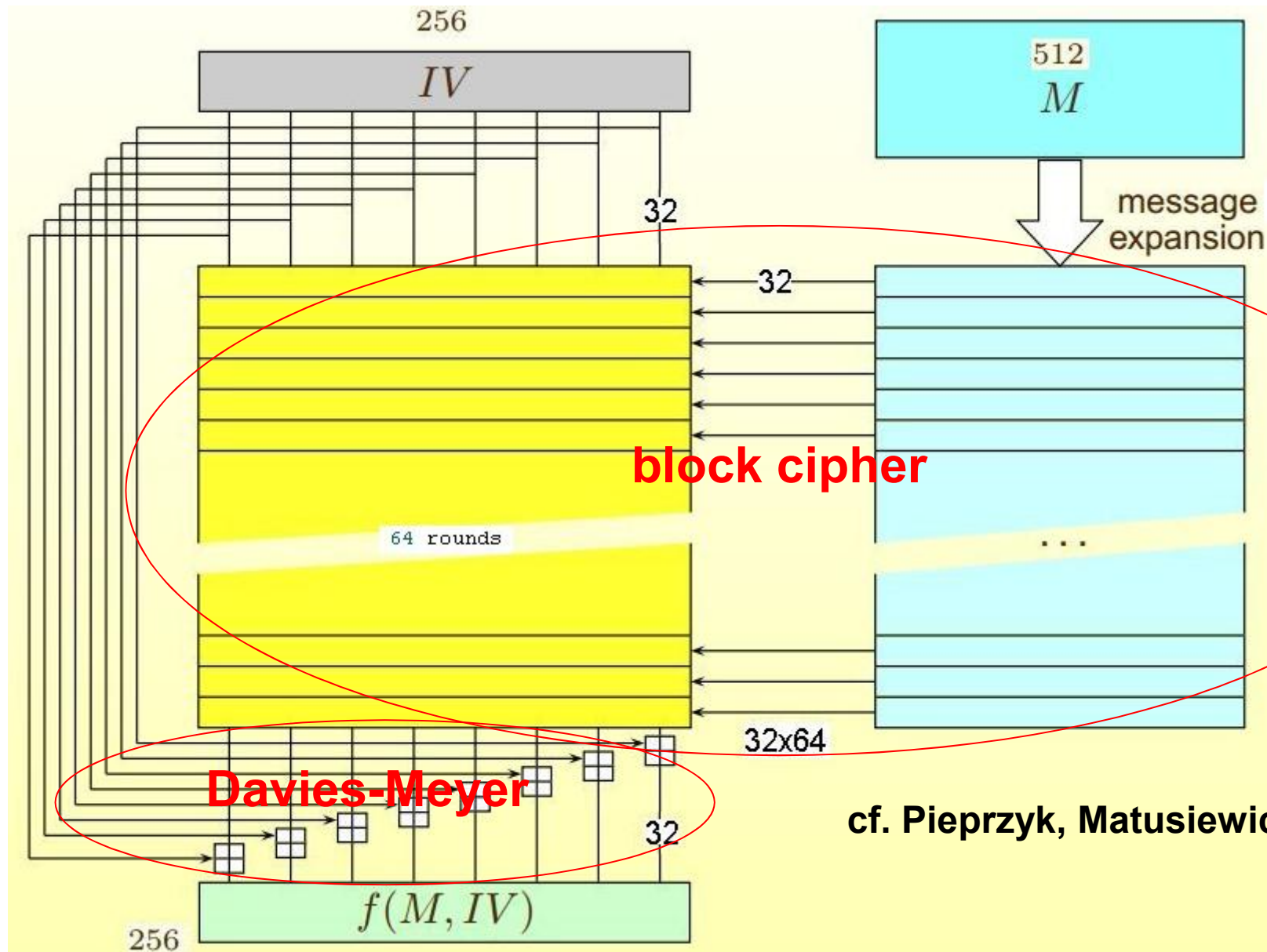


Bitcoin

Hash Functions

And Block Ciphers (!)

SHA-256 Compression Function

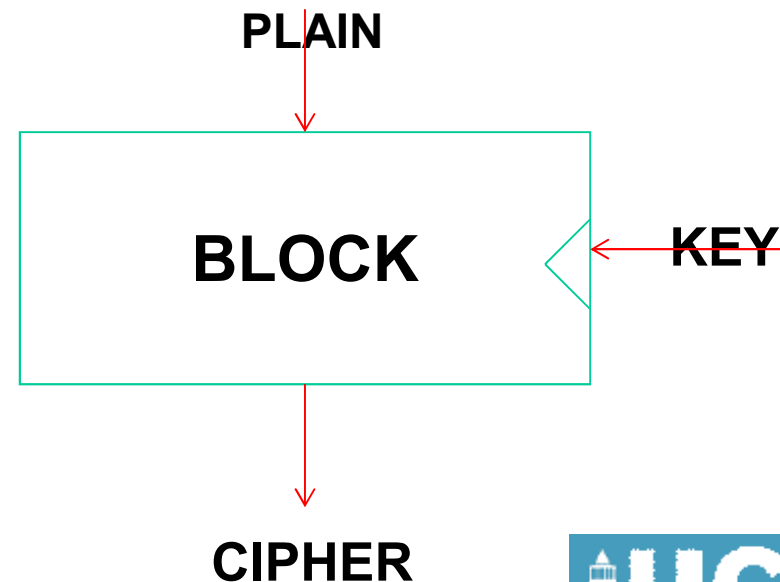


cf. Pieprzyk, Matusiewicz et al.

Fact:

The process of BitCoin Mining is no different than **a brute force attack on a block cipher**:

- Apply the same box many times, with different keys...
- Here the block cipher is a part of a hash function but it does NOT matter.
 - 98% of computational effort is evaluating this block cipher box with various keys and various inputs
 - Like a random oracle.

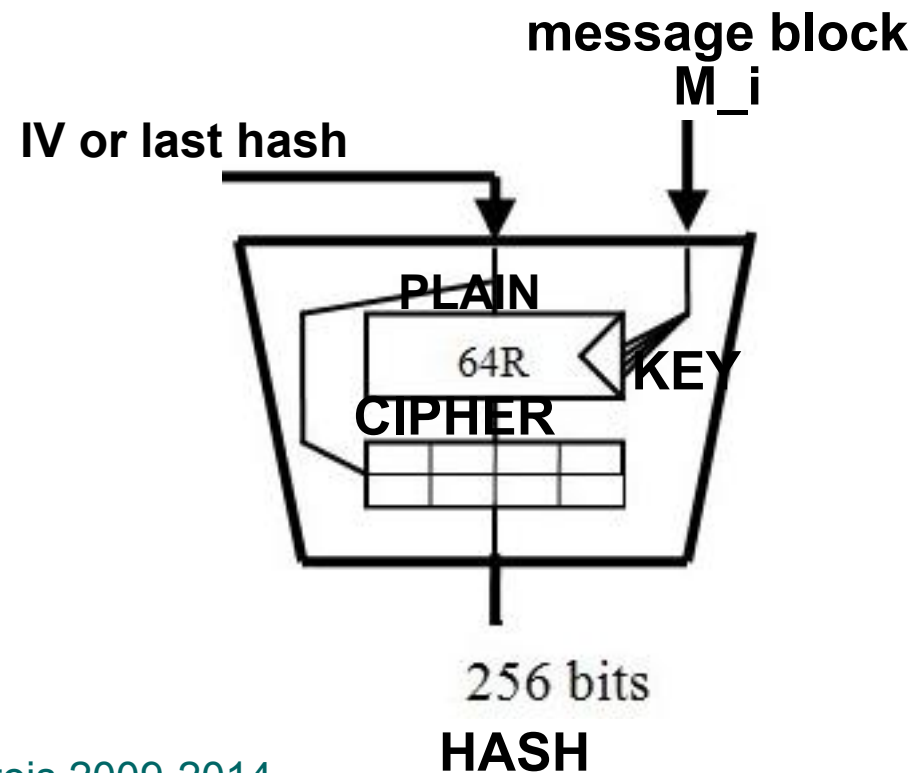


Davies-Meyer

Transforms a block cipher into a hash function.

In SHA-256 we have:

block size=256, 64 rounds, key size=256 expanded 4x.



***One Round of SHA-256

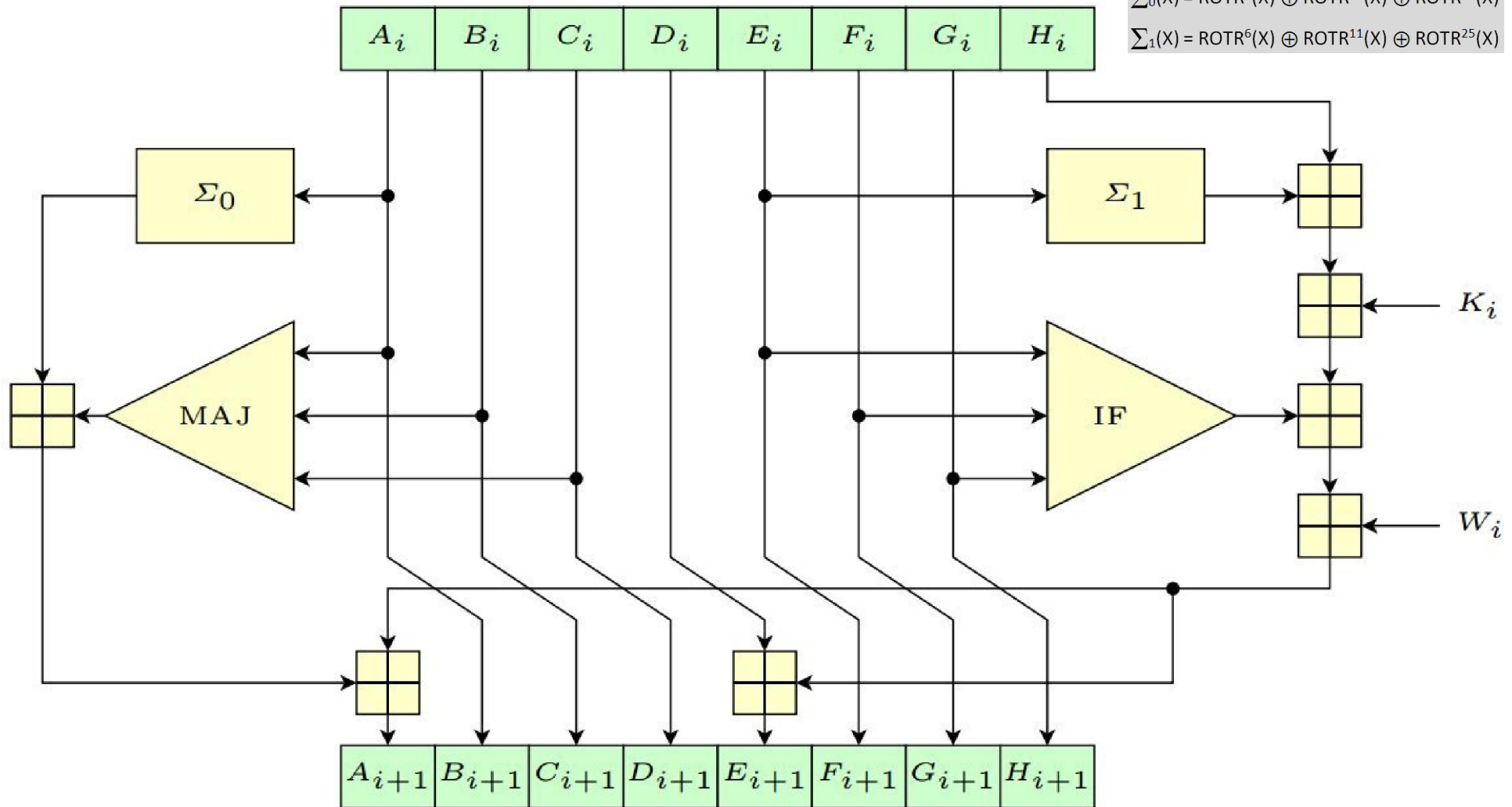
cf. Pieprzyk, Matusiewicz et al.

$$\text{Ch}(X, Y, Z) = (X \wedge Y) \oplus (\neg X \wedge Z)$$

$$\text{Maj}(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$$

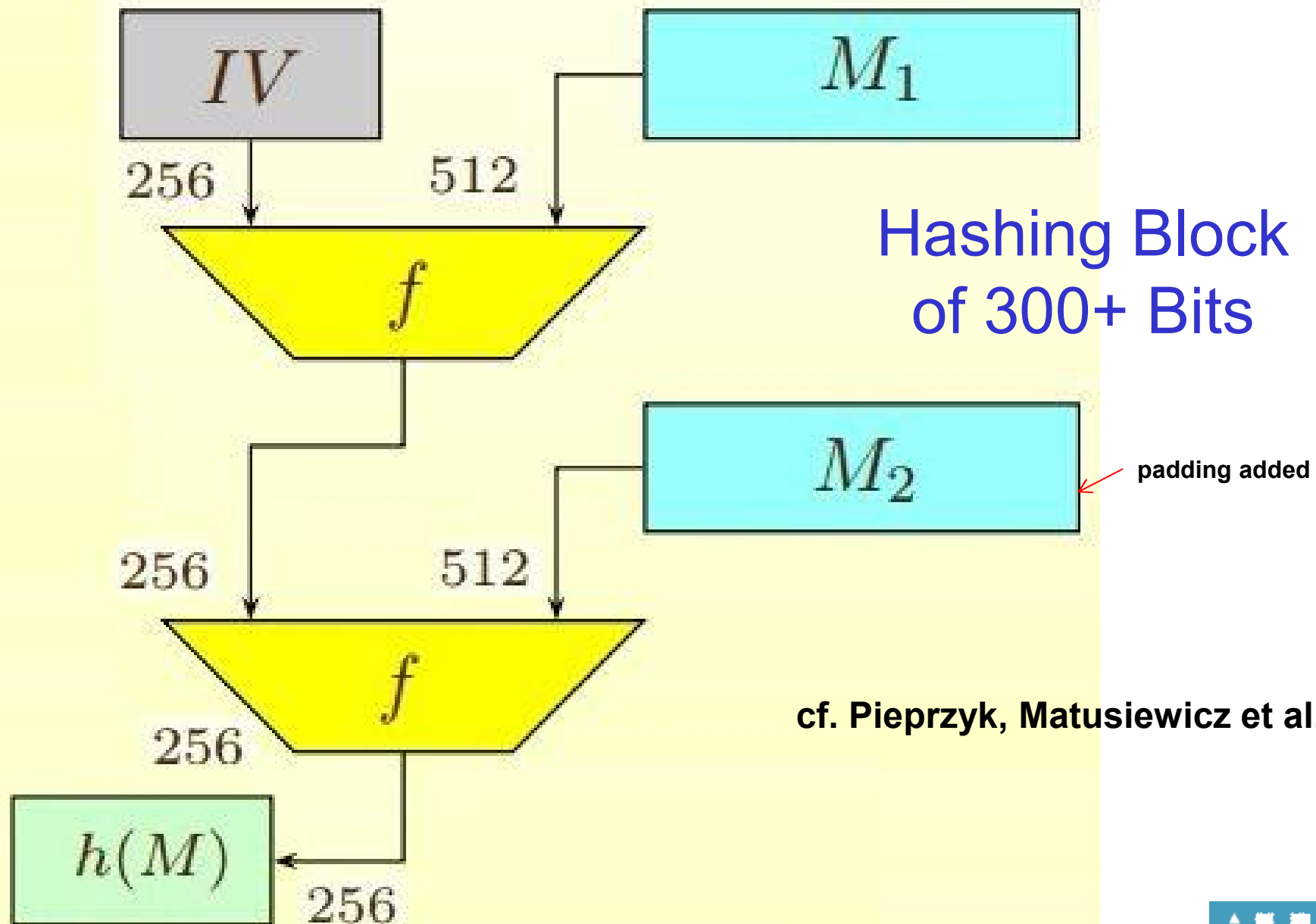
$$\Sigma_0(X) = \text{ROTR}^2(X) \oplus \text{ROTR}^{13}(X) \oplus \text{ROTR}^{22}(X)$$

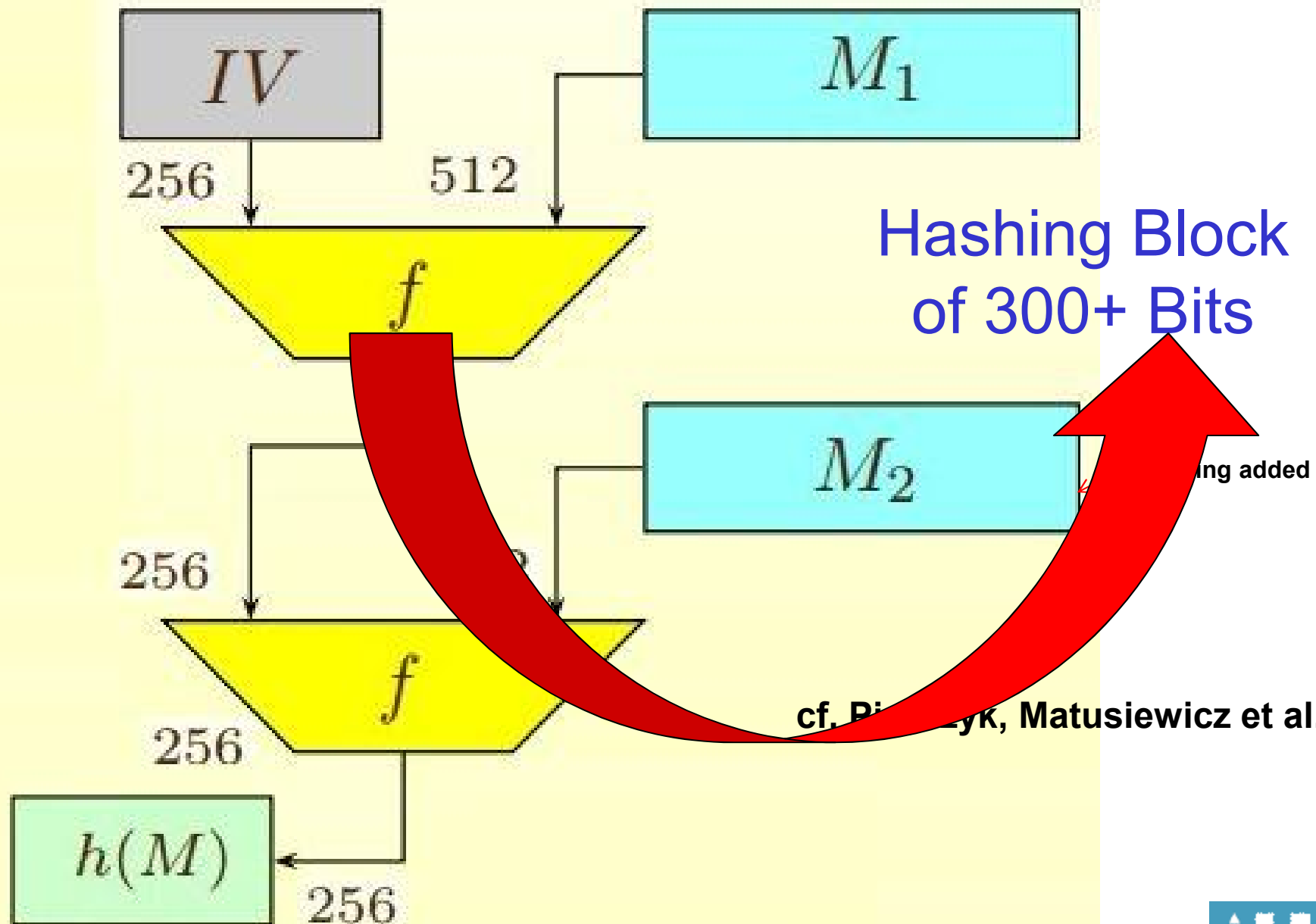
$$\Sigma_1(X) = \text{ROTR}^6(X) \oplus \text{ROTR}^{11}(X) \oplus \text{ROTR}^{25}(X)$$



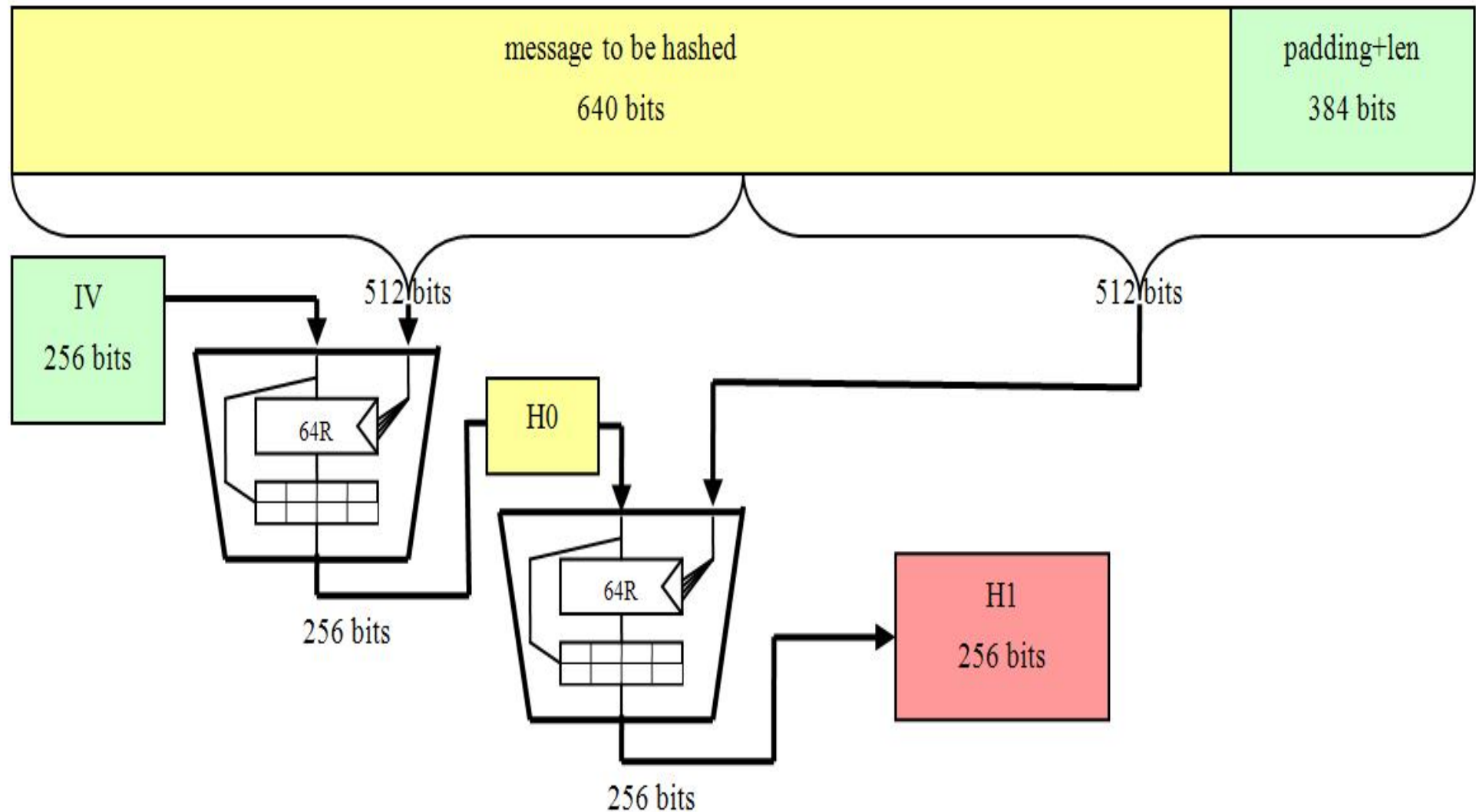
Optimising Mining (39% gain w.r.t. best ASIC) Like Generation 4.1.



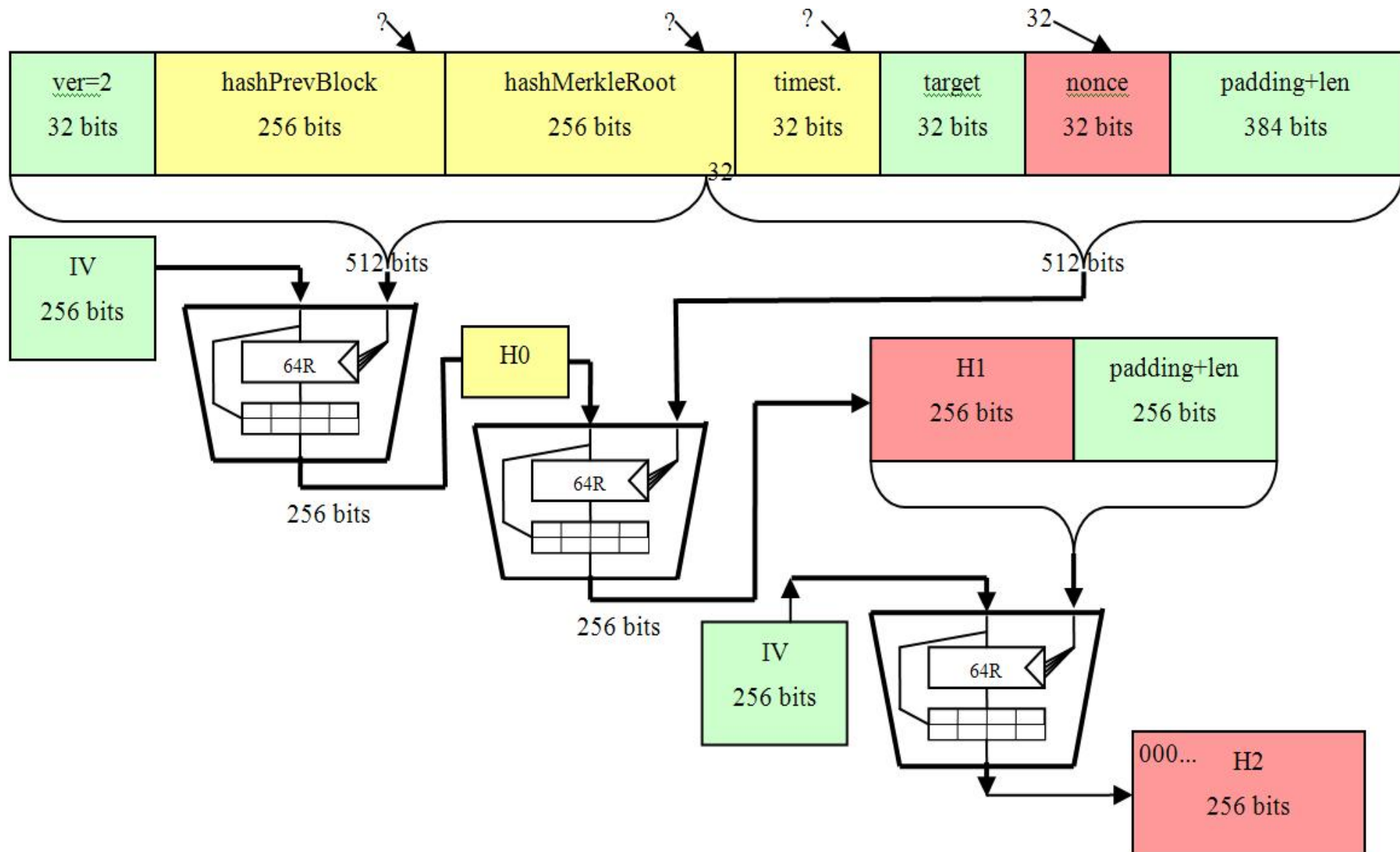




Padding



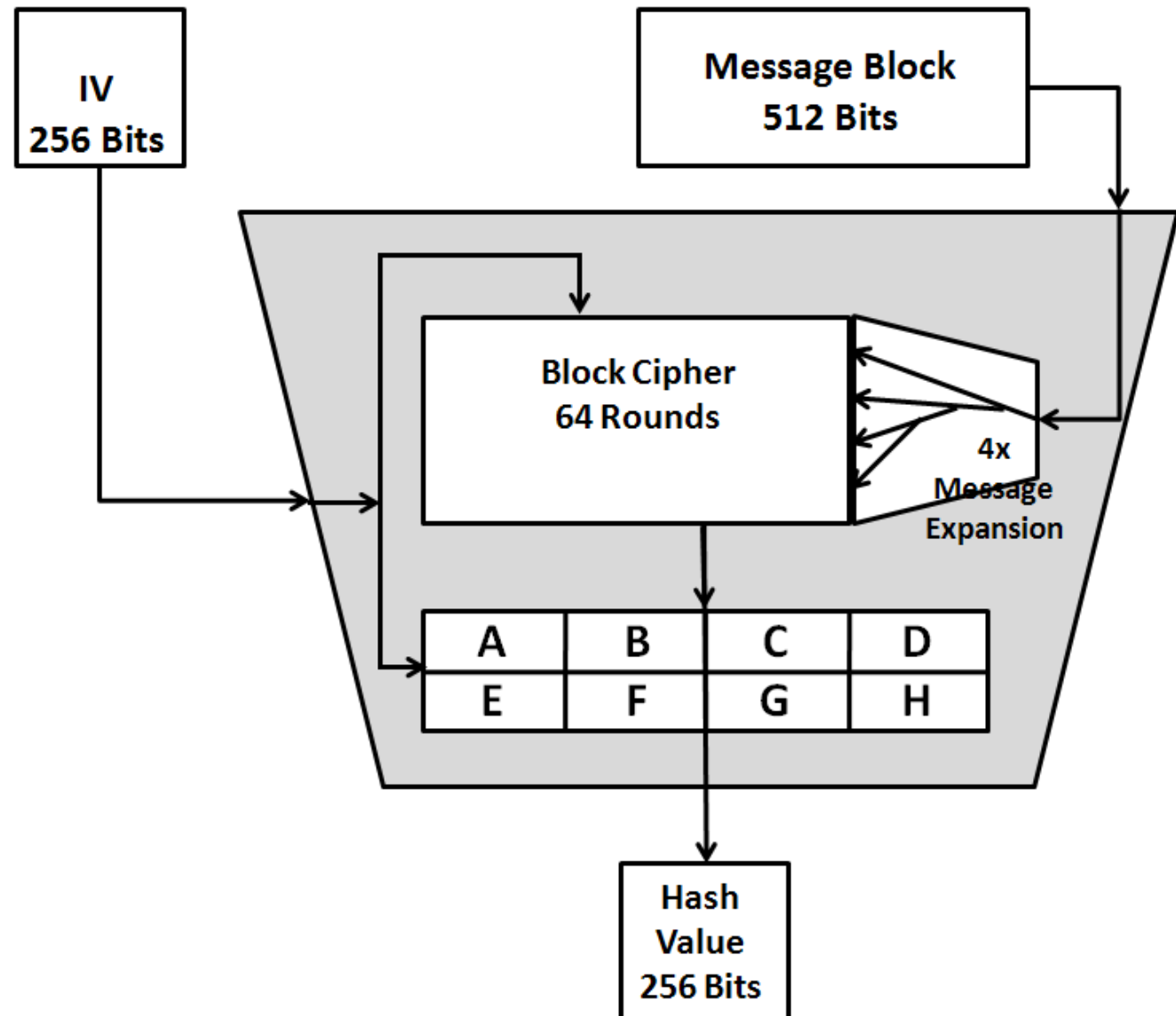
+ Second Hash



Inputs

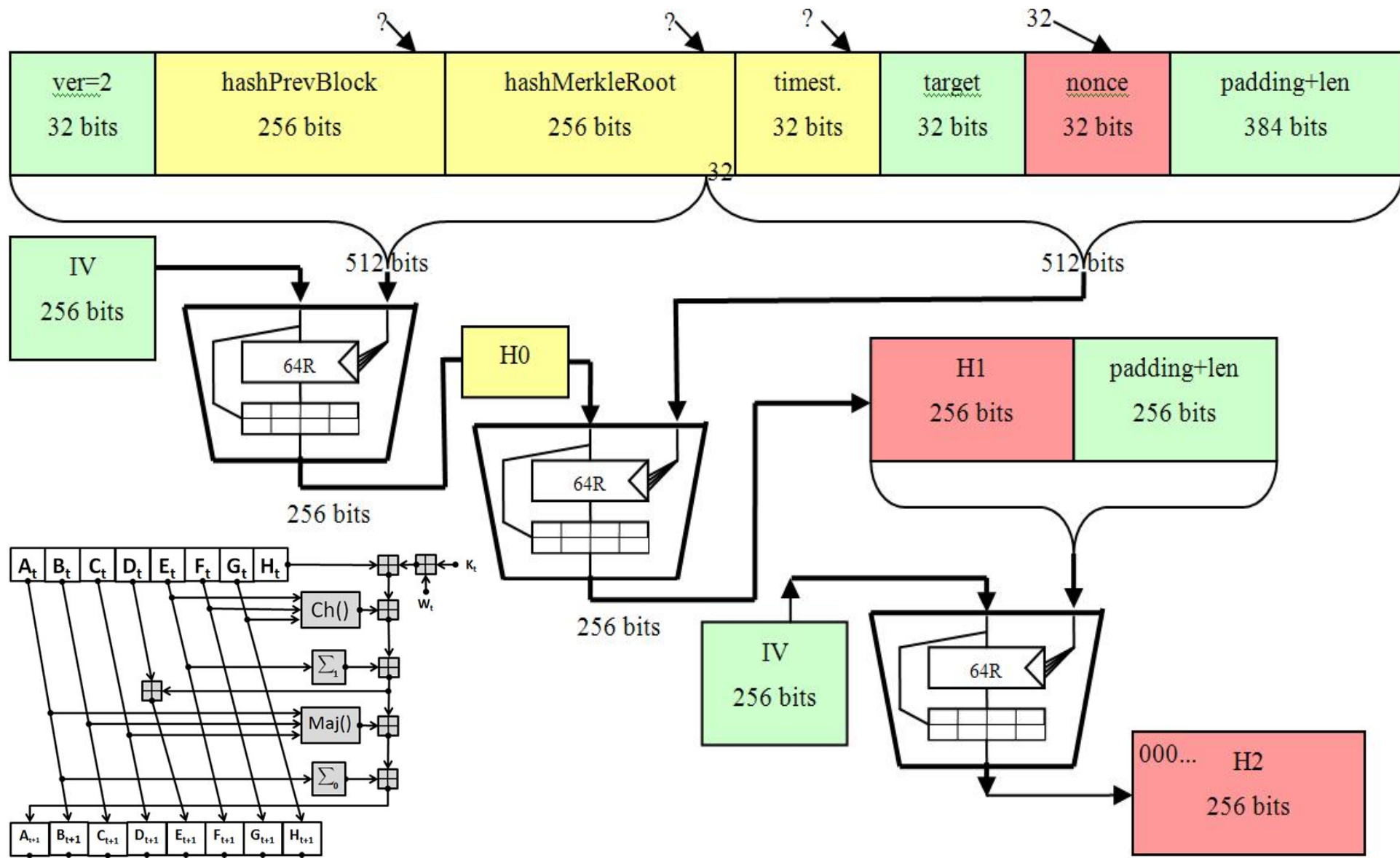
Field	Size	Description
version	32 bits	Version of the Bitcoin software version creating this block
hashPrevBlock	256 bits	Hash of the previous block considered as valid in the Bitcoin network (most of the time there is only one candidate)
hashMerkleRoot	256 bits	Here a set of recent yet unconfirmed Bitcoin transactions are hashed into one single value on 256 bits = the Merkle Root
timestamp	32 bits	Current timestamp in seconds since 1970-01-01 00:00 UTC
target	32 bits	The current Target represented in a compact 32 bit format
nonce	32 bits	Nonce chosen by the miner, typically goes from 0x00000000 to 0xFFFFFFFF until the CISO puzzle is solved
padding + <u>len</u>	384 bits	standard fixed SHA256 padding on 384 bits for Len=640 bits

Davies-Meyer

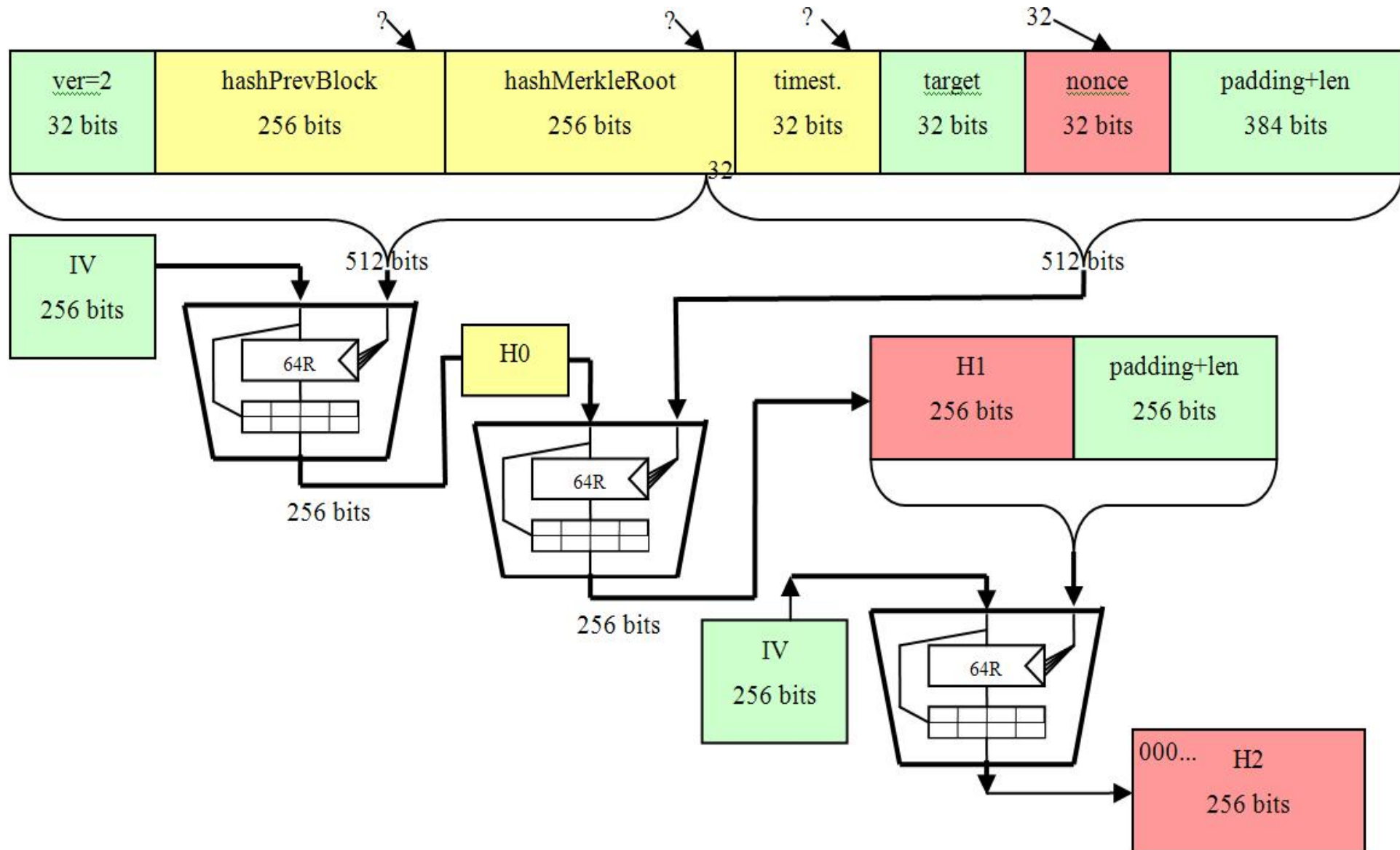


hashed data from
previous transactions

Mining Internals



Improvement 1 – Amortized Cost(H0)=0



Improvement 2 – Gains 3 Rounds At the End

	A	B	C	D	E	F	G	H
t=59:	B6AE8FFF	FFB70472	C062D46F	FCD1887B	B21BAD3D	6D83BFC6	7E44008E	9B5E906C
t=60:	B85E2CE9	B6AE8FFF	FFB70472	C062D46F	961F4894	B21BAD3D	6D83BFC6	7E44008E
t=61:	04D24D6C	B85E2CE9	B6AE8FFF	FFB70472	948D25B6	961F4894	B21BAD3D	6D83BFC6
t=62:	D39A2165	04D24D6C	B85E2CE9	B6AE8FFF	FB121210	948D25B6	961F4894	B21BAD3D
t=63:	506E3058	D39A2165	04D24D6C	B85E2CE9	5EF50F24	FB121210	948D25B6	961F4894

Improvement 3

—
Gains
3 Rounds
At the
Beginning

—
they do NOT depend
on the nonce

computation of H1		
Round t	32 bit W_t	Description
0	XXXXXXXX	last 32 Bits of hashMerkleRoot
1	XXXXXXXX	timestamp
2	XXXXXXXX	target
3	XXXXXXXX	nonce (00000000 to FFFFFFFF)
4	0x80000000	padding starts
5	0x00000000	
6	0x00000000	
7	0x00000000	
8	0x00000000	
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	padding ends
14	0x00000000	length H
15	0x00000280	length L

computation of H2		
Round t	32 bit W_t	Description
0	XXXXXXXX	$H1_0$
1	XXXXXXXX	$H1_1$
2	XXXXXXXX	$H1_2$
3	XXXXXXXX	$H1_3$
4	XXXXXXXX	$H1_4$
5	XXXXXXXX	$H1_5$
6	XXXXXXXX	$H1_6$
7	XXXXXXXX	$H1_7$
8	0x80000000	Padding Starts
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	Padding Ends
14	0x00000000	length H
15	0x00000100	length L

Improvement 4

— Incremental Computation

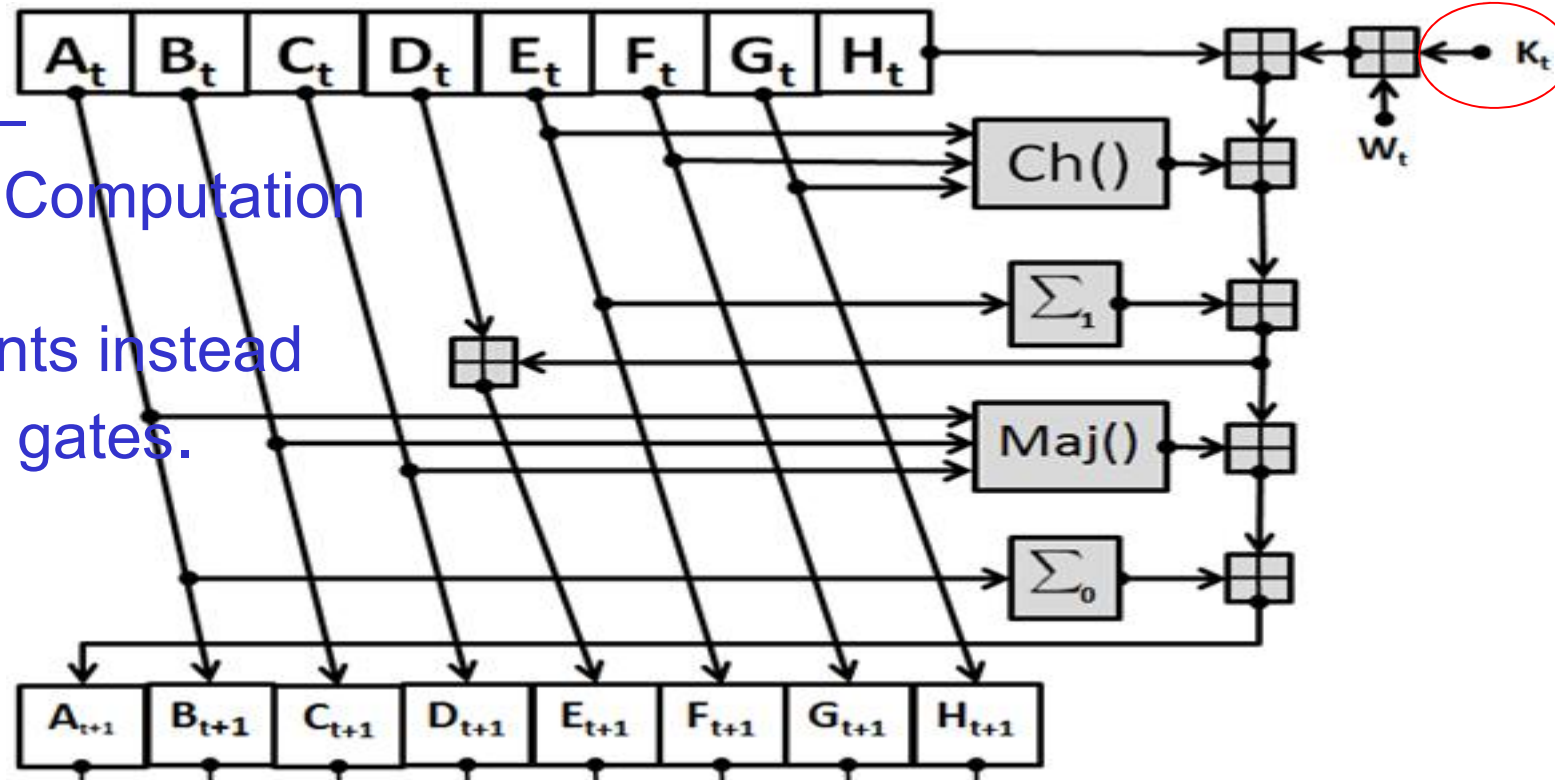
computation of H1		
Round t	32 bit W_t	Description
0	XXXXXXXX	last 32 Bits of hashMerkleRoot
1	XXXXXXXX	timestamp
2	XXXXXXXX	target
3	XXXXXXXX	nonce (00000000 to FFFFFFFF)
4	0x80000000	padding starts
5	0x00000000	
6	0x00000000	
7	0x00000000	
8	0x00000000	
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	padding ends
14	0x00000000	length H
15	0x00000280	length L

computation of H2		
Round t	32 bit W_t	Description
0	XXXXXXXX	$H1_0$
1	XXXXXXXX	$H1_1$
2	XXXXXXXX	$H1_2$
3	XXXXXXXX	$H1_3$
4	XXXXXXXX	$H1_4$
5	XXXXXXXX	$H1_5$
6	XXXXXXXX	$H1_6$
7	XXXXXXXX	$H1_7$
8	0x80000000	Padding Starts
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	Padding Ends
14	0x00000000	length H
15	0x00000100	length L

Improvement 4 - contd

Incremental Computation

2 increments instead
of 200 gates.



Nonce	A	B	C	D	E	F	G	H
0x00000000	c14c28c6	fdd86aa7	1184d36	2703413e	346785c7	c1abdbc7	8f925db9	a4b56f21
0x00000001	c14c28c7	fdd86aa7	1184d36	2703413e	346785c8	c1abdbc7	8f925db9	a4b56f21
0x00000002	c14c28c8	fdd86aa7	1184d36	2703413e	346785c9	c1abdbc7	8f925db9	a4b56f21
0x00000003	c14c28c9	fdd86aa7	1184d36	2703413e	346785ca	c1abdbc7	8f925db9	a4b56f21
0x00000004	c14c28ca	fdd86aa7	1184d36	2703413e	346785cb	c1abdbc7	8f925db9	a4b56f21
0x00000005	c14c28cb	fdd86aa7	1184d36	2703413e	346785cc	c1abdbc7	8f925db9	a4b56f21

$$Ch(X, Y, Z) = (X \wedge Y) \oplus (\neg X \wedge Z)$$

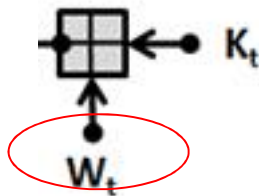
$$Maj(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$$

$$\Sigma_0(X) = ROTR^2(X) \oplus ROTR^{13}(X) \oplus ROTR^{22}(X)$$

$$\Sigma_1(X) = ROTR^6(X) \oplus ROTR^{11}(X) \oplus ROTR^{25}(X)$$

Improvement 5

—
Gains
18 Additions
≈ 3600 gates



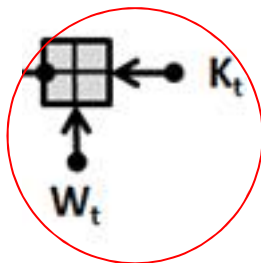
computation of H1		
Round t	32 bit W_t	Description
0	XXXXXXXX	last 32 Bits of hashMerkleRoot
1	XXXXXXXX	timestamp
2	XXXXXXXX	target
3	XXXXXXXX	nonce (00000000 to FFFFFFFF)
4	0x80000000	padding starts
5	0x00000000	
6	0x00000000	
7	0x00000000	
8	0x00000000	
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	padding ends
14	0x00000000	length H
15	0x00000280	length L

computation of H2		
Round t	32 bit W_t	Description
0	XXXXXXXX	$H1_0$
1	XXXXXXXX	$H1_1$
2	XXXXXXXX	$H1_2$
3	XXXXXXXX	$H1_3$
4	XXXXXXXX	$H1_4$
5	XXXXXXXX	$H1_5$
6	XXXXXXXX	$H1_6$
7	XXXXXXXX	$H1_7$
8	0x80000000	Padding Starts
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	Padding Ends
14	0x00000000	length H
15	0x00000100	length L

Improvement 6

—
 Saving
 2 More Additions
 ≈ 400 gates
 with Hard Coding

AND SAVE LIKE HALF
 of the next addition!
 (addition with a constant = cheaper,
 depends on the constant)

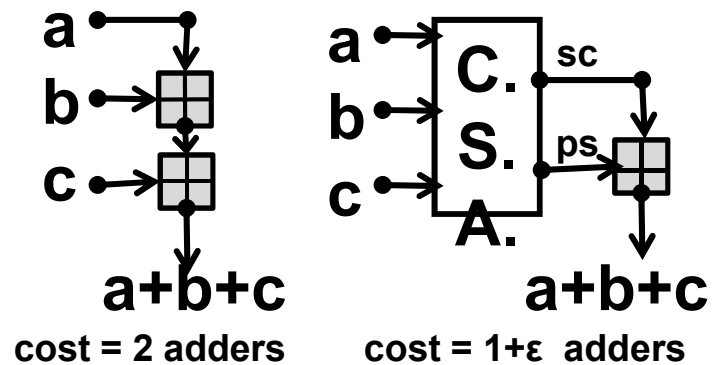


computation of H1		
Round t	32 bit W_t	Description
0	XXXXXXXX	last 32 Bits of hashMerkleRoot
1	XXXXXXXX	timestamp
2	XXXXXXXX	target
3	XXXXXXXX	nonce (00000000 to FFFFFFFF)
4	0x80000000	padding starts
5	0x00000000	
6	0x00000000	
7	0x00000000	
8	0x00000000	
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	padding ends
14	0x00000000	length H
15	0x00000280	length L

computation of H2		
Round t	32 bit W_t	Description
0	XXXXXXXX	$H1_0$
1	XXXXXXXX	$H1_1$
2	XXXXXXXX	$H1_2$
3	XXXXXXXX	$H1_3$
4	XXXXXXXX	$H1_4$
5	XXXXXXXX	$H1_5$
6	XXXXXXXX	$H1_6$
7	XXXXXXXX	$H1_7$
8	0x80000000	Padding Starts
9	0x00000000	
10	0x00000000	
11	0x00000000	
12	0x00000000	
13	0x00000000	Padding Ends
14	0x00000000	length H
15	0x00000100	length L

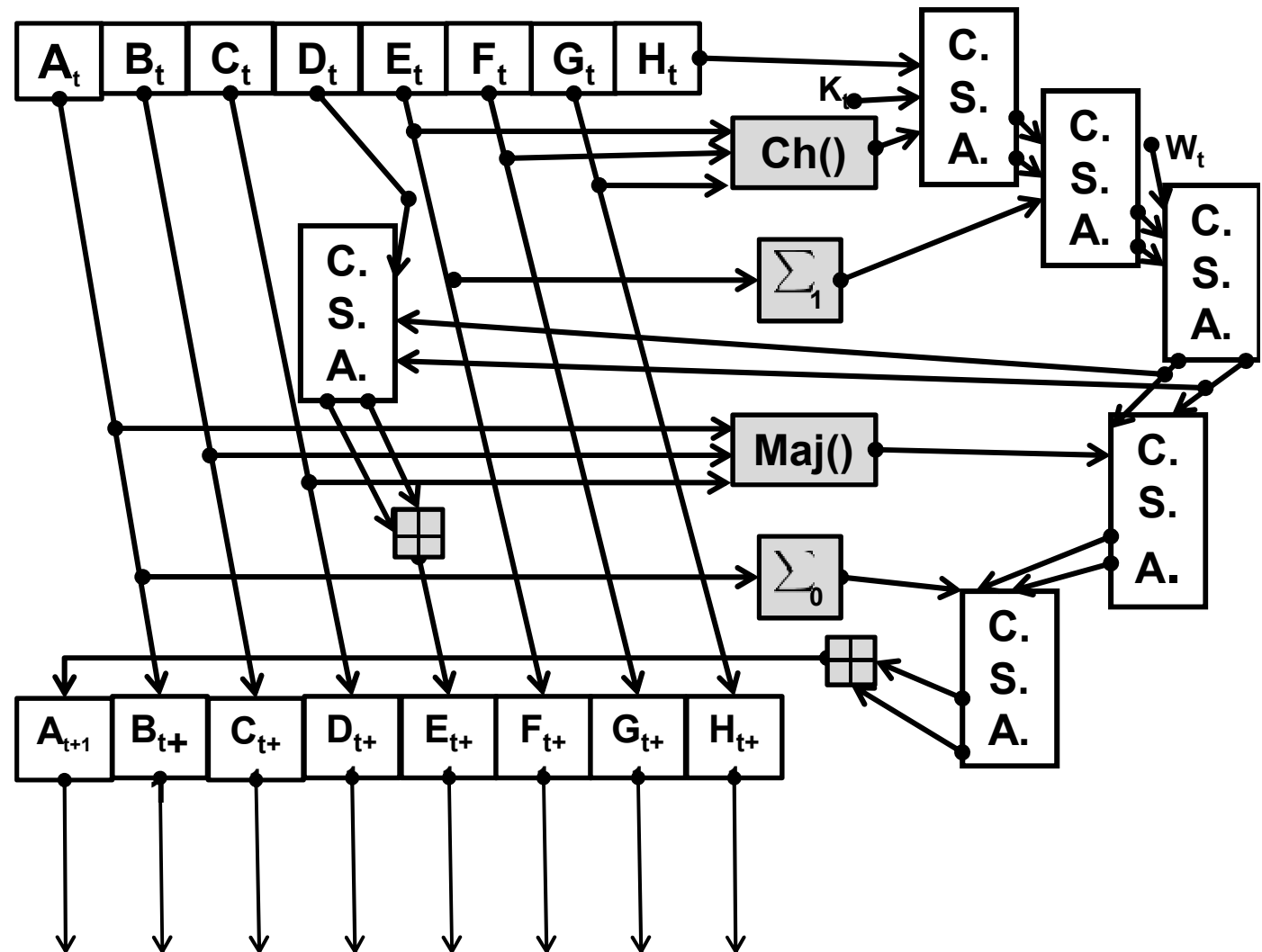
Improvement X

Classical trick: Carry Save Adders.



Whole Round

Only **two** full adders.



Message Schedule

For $0 \leq t \leq 15$,

$W_t = M_t$ **=> just copy for 16 R**

For $16 \leq t \leq 63$, **non-trivial part**

$$W_t = \sigma_1(W_{t-2}) \boxplus W_{t-7} \boxplus \sigma_0(W_{t-15}) \boxplus W_{t-16}$$

$$\sigma_0(x) = \text{ROTR}^7(x) \oplus \text{ROTR}^{18}(x) \oplus \text{SHR}^3(x)$$

$$\sigma_1(x) = \text{ROTR}^{17}(x) \oplus \text{ROTR}^{19}(x) \oplus \text{SHR}^{10}(x)$$

$$\sigma_0(x) = \text{ROTR}^7(x) \oplus \text{ROTR}^{18}(x) \oplus \text{SHR}^3(x)$$

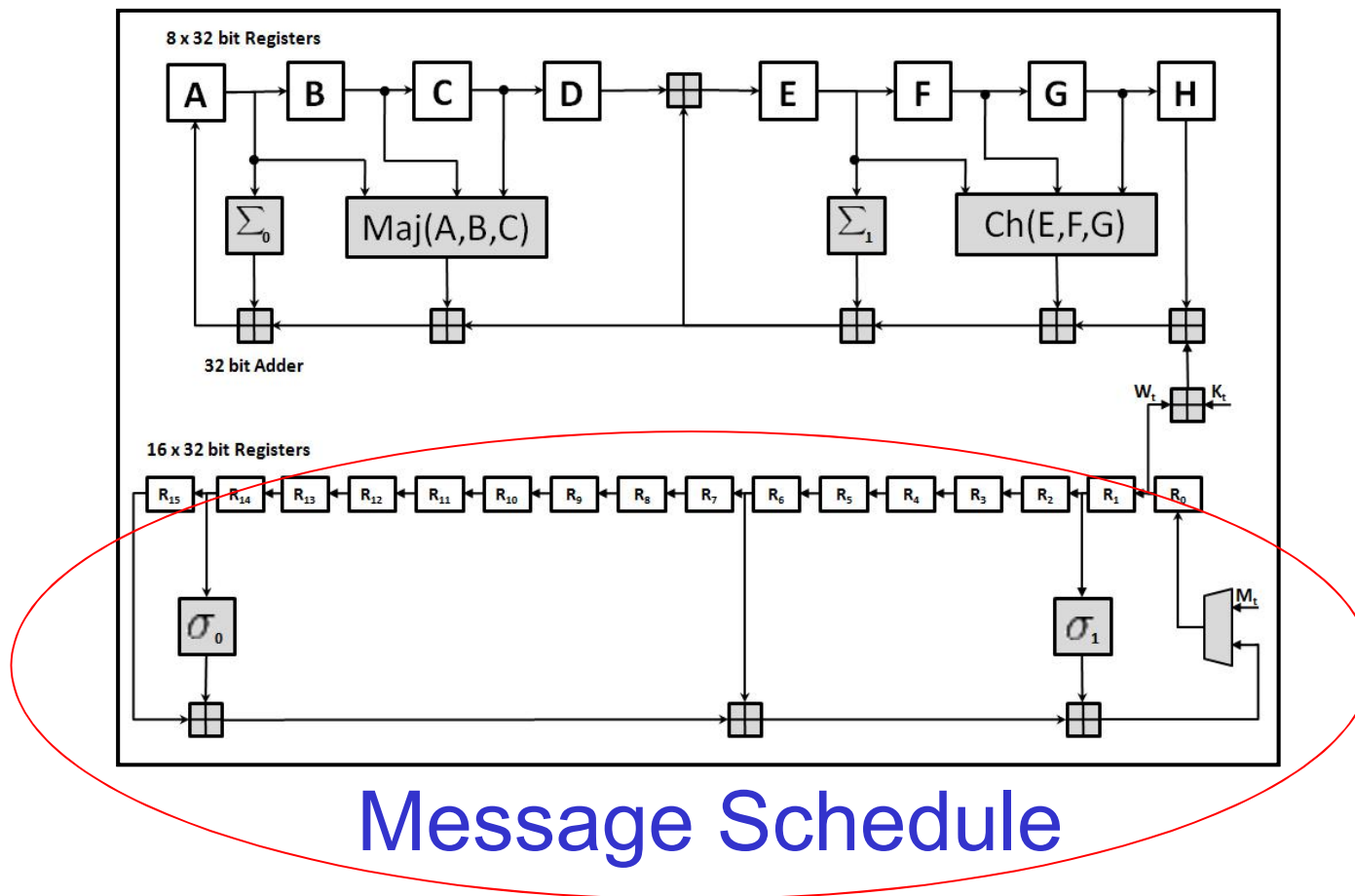
$$\sigma_1(x) = \text{ROTR}^{17}(x) \oplus \text{ROTR}^{19}(x) \oplus \text{SHR}^{10}(x)$$

$$\text{Ch}(X, Y, Z) = (X \wedge Y) \oplus (\neg X \wedge Z)$$

$$\text{Maj}(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$$

$$\Sigma_0(X) = \text{ROTR}^2(X) \oplus \text{ROTR}^{13}(X) \oplus \text{ROTR}^{22}(X)$$

$$\Sigma_1(X) = \text{ROTR}^6(X) \oplus \text{ROTR}^{11}(X) \oplus \text{ROTR}^{25}(X)$$



Improvement 7 - Fact:

Some early values do NOT yet depend on the **nonce**.
In H1 computation only (left column).

$$W_{16} = \sigma_1(W_{14}) \boxplus W_9 \boxplus \sigma_0(W_1) \boxplus W_0$$

$$W_{17} = \sigma_1(W_{15}) \boxplus W_{10} \boxplus \sigma_0(W_2) \boxplus W_1$$

Improvement 7 – 3 more

2 more 32-bit additions are saved by hard coding,

and more for the next addition

(again, adding a constant, depends on the constant, average cost maybe saving another 1? addition).

Some 600 extra gates saved.

Improvement 8 – 1 More Incremental

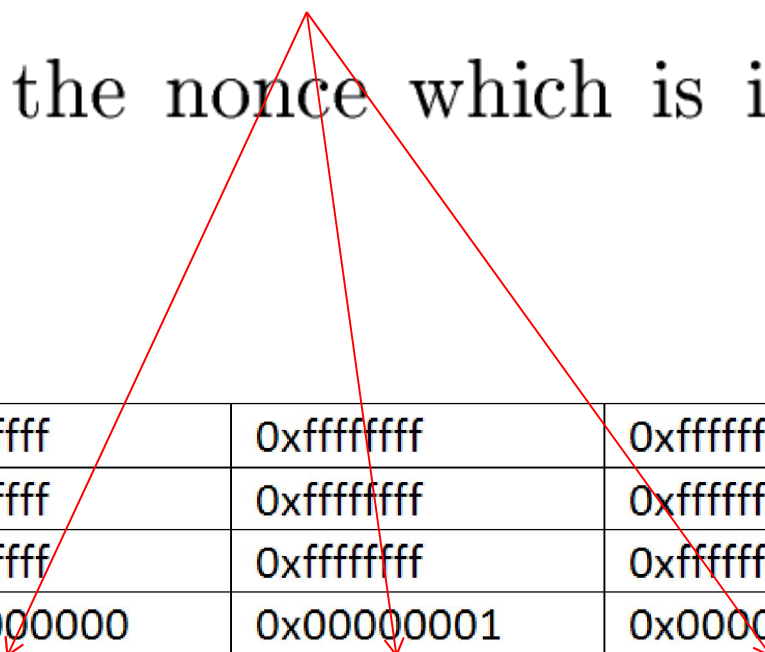
We have:

nonce



$$W_{19} = \sigma_1(W_{17}) \boxplus W_{11} \boxplus \sigma_0(W_4) \boxplus W_3.$$

W_3 is the nonce which is incremented by 1



W_0	0xffffffff	0xffffffff	0xffffffff	0xffffffff	0xffffffff
W_1	0xffffffff	0xffffffff	0xffffffff	0xffffffff	0xffffffff
W_2	0xffffffff	0xffffffff	0xffffffff	0xffffffff	0xffffffff
W_3	0x00000000	0x00000001	0x00000002	0x00000003	0x00000004
W_{19}	0x1108b759	0x1108b75a	0x1108b75b	0x1108b75c	0x1108b75d

Table 9: Code Execution Results for W_{19} with Different Nonces

Improvement X2

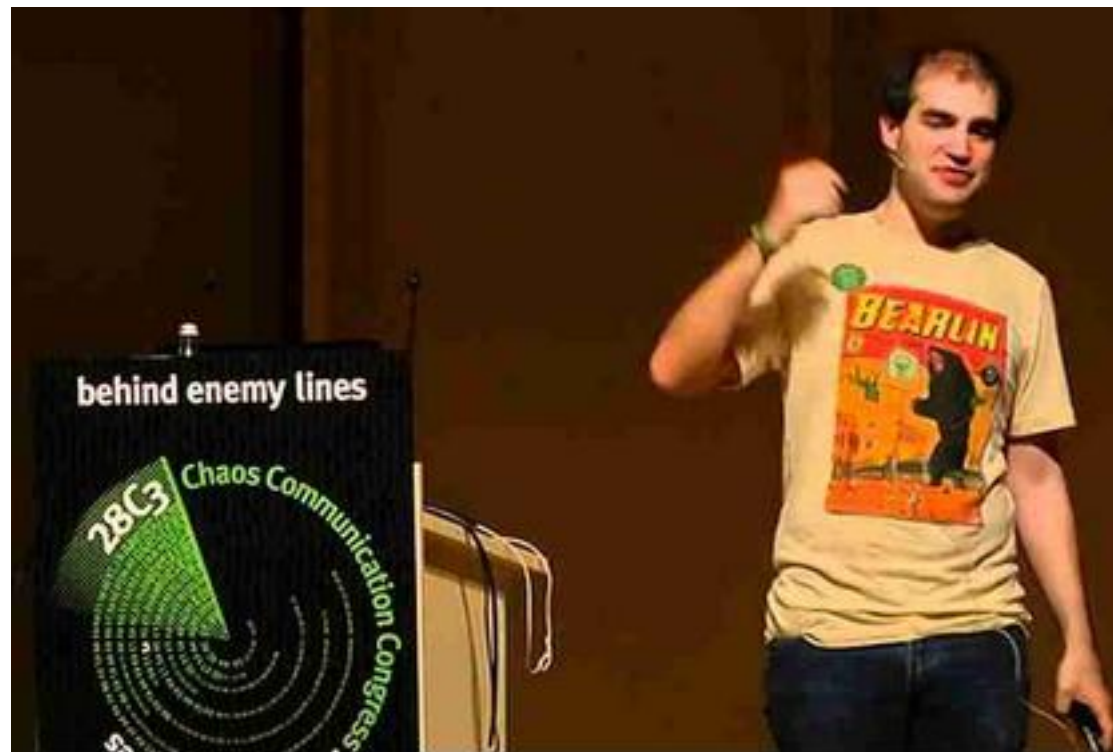
Also use Carry Save Adders in message scheduling.

Only 1 full adder in each of (only) $48-3$ values which need still to be computed.

Optimising The Mining

Fact 12.1 (Hash Speed). The amortized average cost of trying one output H_2 to see if it is likely to have 60 or more leading zeros is at most about 1.89 computations of the compression function of SHA-256 instead of 3.0, which represents an improvement by 39%.

Future – Dan Kaminsky



San Diego Bitcoin Conference May 2013

Earlier he said that he has no stakes in 'this game'.

Then at minute 40 he claims that **the current Bitcoin Proof of Work function based on SHA-256 will not survive "the year"** (to be replaced before end of 2013). He says that **assigns zero percent probability that "we" will continue with the present POW function**". Back to CPU mining.

<https://www.youtube.com/watch?v=si-2niFDgtI>

Security Panel - **Bitcoin** 2013 Confernece - YouTube



www.youtube.com/watch?v=si-2niFDgtI ▼

May 29, 2013 - Uploaded by Lindsay Holland

... Hoffman, **Dan Kaminsky** discuss **Bitcoin** security at the **Bitcoin 2013 Conference** ... in **San Jose**, California, May 18, 2013, hosted by the **Bitcoin** Foundation. ... **Bitcoin 2013 conference** - Greg Broiles - Nuts and Bolts of **Bitcoin** ...

SHA-256 to be phased out?

<https://www.youtube.com/watch?v=si-2niFDgtI>



HOWEVER:

NOBODY OWNS BITCOIN

We claim the contrary: any attempt to change the POW is close to impossible to enforce AND if mandated by some group of people, it will lead to **a SPLIT IN THE BITCOIN COMMUNITY.**

An organised divorce of people and software developers who will be **running two separate block chain** versions.

I Was Proven Right

1.5 years later it has NOT been changed.

Too much money at stake.

Other Related Research

[Sergio Demian Lerner]

see

blog.bettercrypto.com/?p=1874

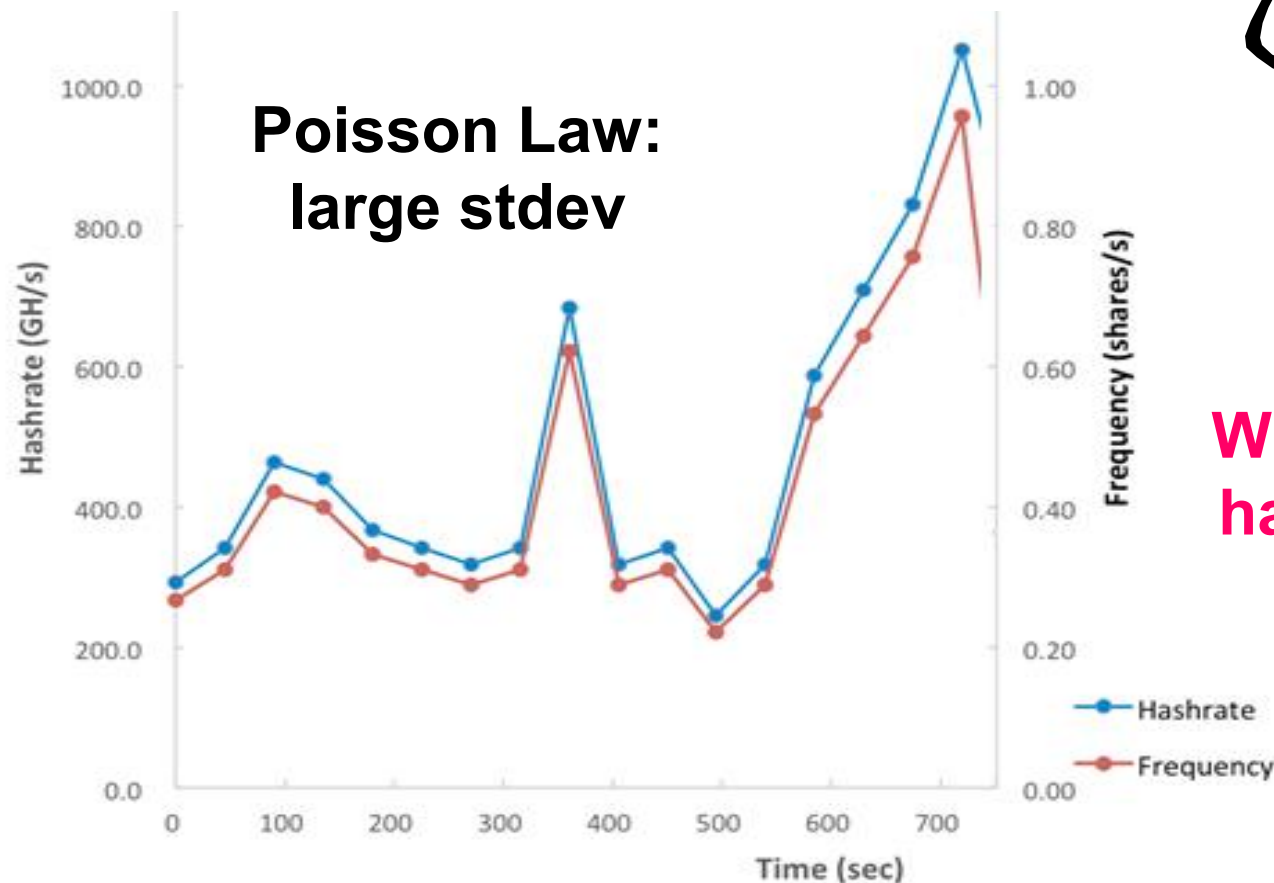
Mining In Pools



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?**

Why Pools?



Reason 2. Huge Incertitudes:

Law Of Bitcoin Mining: It follows the Poisson Distribution:

- If for example in 1 month the miner expect to find 4 blocks, the standard deviation is about $\sqrt{4}=2$.
- In one month he will find 6 in some months he will find 2, sometimes he will find 0.

VERY STRESSFUL. Cannot sleep at night.

- Does my miner work correctly??? Wait for 10 years to see...
- Are other miners cheating? Am I getting a fair share???
 - [YES, as we will see later miners can cheat and earn more than other miners]

What Are Pools?

- A group of small/larger miners who work together. Also protects their anonymity, also a social dimension:
- Effectively a cooperative: can provide support, mentoring, shared hosting, stats, management apps etc...
- Beware: 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%.

They have publicly said: please leave, do not join.

- 50% attack = total control of bitcoin by one single entity.

pool	<i>percentage</i>
BTCGuild.com	26%
GHash.io	40%
Eligius.st	10%
Bitcoin.cz	6%
Bitminter.com	5%

Ukraine,
moved to
UK

Pools Operation

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

Answer: Probably There Isn't.

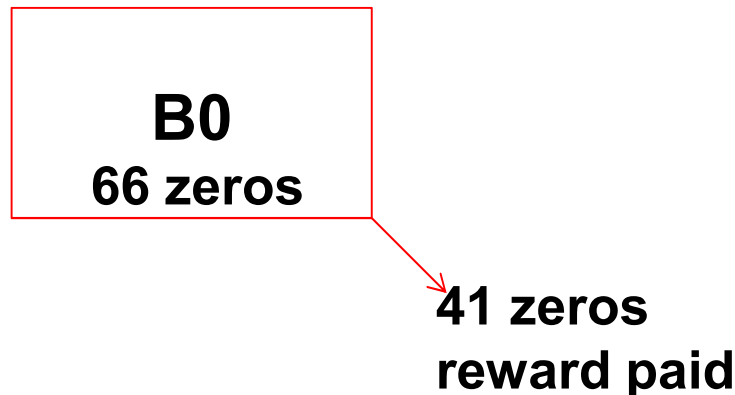
There is already ample literature on this.

Bitcoin Share

A proof of effort: allows one to be paid.

=def= A hash starting with 41 zeros (one in 2^{41} hashes).

Typical value, can be 40 or 43. We obtain $41=32+9$ when difficulty= 2^9 .



Why difficulty= $2^9=512$?

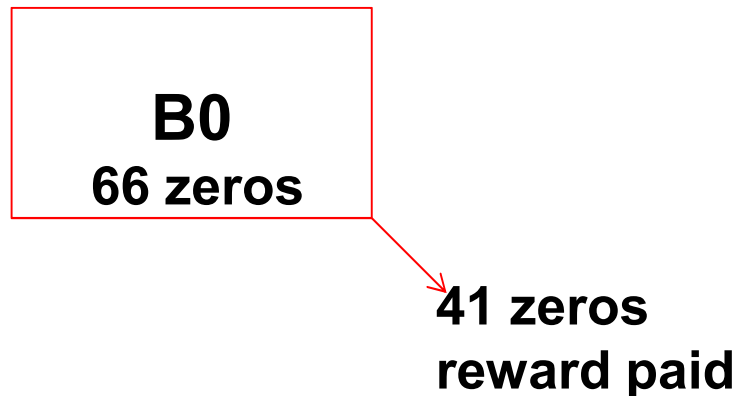
Optimal value was chosen by your pool manager in order to keep server bandwidth and load reasonable, yet have good precision measuring your contributed hash power (more smaller events=>low variance).

Can change in real time if the server cannot cope with current load, or you hash rate is upgraded.

Bitcoin Share

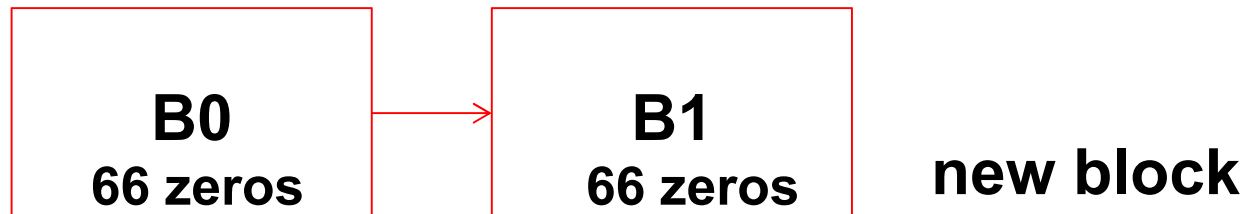
A proof of effort: allows one to be paid.

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



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

$$66 = 41 + 25$$



Trouble With Mining Management

Q: How to prevent people from hiding their “winning ticket” from the pool? Maybe embed information about “the pool” inside each potential block data. Not enough:

*Solution 1: Mine with a private key known to individual miners?

⇒ Allows all miners to cheat.

⇒ We would need to trust the network (e.g. other miners) not to accept this block outside of the pool. Seems impossible.

Solution 2: Mine with a **private key not known to individual miners!**

⇒ **Allows the pool manager to steal the money. Must be trusted.**

⇒ **BTW. This risk is mitigated by frequent pay-outs**

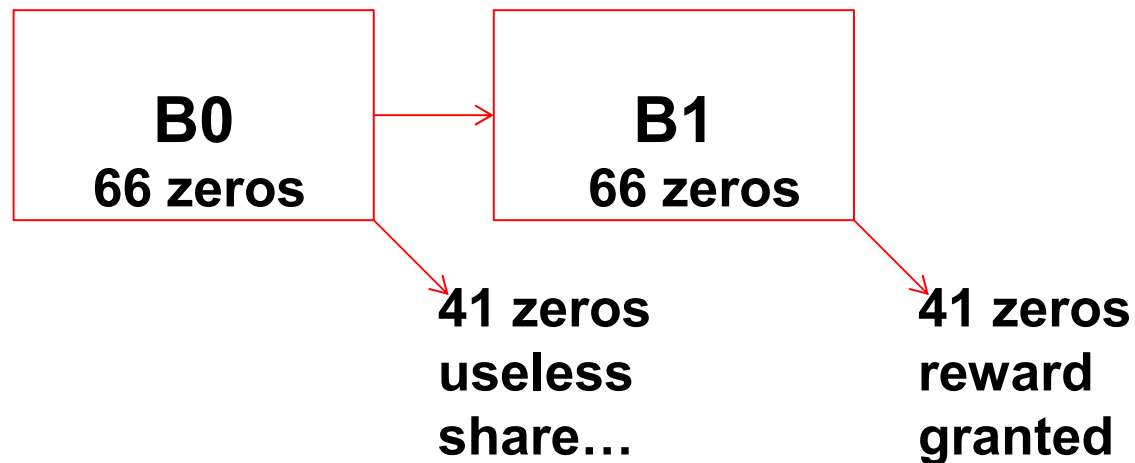
⇒ The only plausible solution in existence.

*Stale/Rejected Shares

No precise definition,

Used when large quantities of shares out of date are produced,
problem in a pool where miners have not been notified that
their work is out of date.

(it might however re-become good later) due to fork situations.



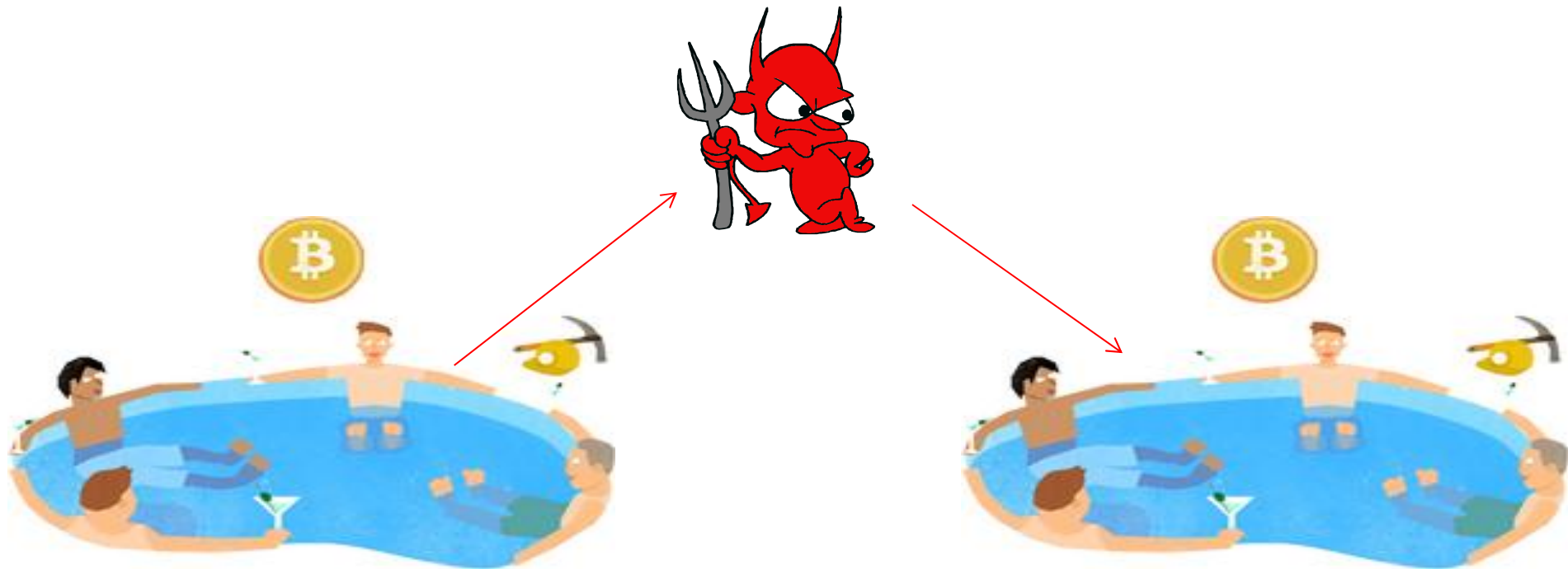
****Dupe Shares**

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...

Attacks:

Pool Hopping Attack



Pool Hopping

The "Pool Hopping Attack" was amply studied by Rosenfeld
It allows malicious miners to obtain gains which are in
proportion higher than their fair share.

How?

Remember the pools work like a lottery, a group of people plays
together for up to 1 winning ticket to share.

Pool Hopping – Main Idea

If a miner mines in a pool in which a lot of shares have already been submitted and no block has yet been found, he will gain less in expectation because the reward will be shared with the miners who have contributed to this pool.

Therefore at a certain moment it may be profitable to stop mining in this pool and contribute elsewhere (reward will be shared with less people).

This remains valid even if the pools penalize leavers and refuse to pay for their contribution if they do not mine for a complete ``shift". It is still profitable for miners to quit and mine for another pool (or mine independently).

Pool Hopping – Defenses

This attack works more or less well depending on how exactly pools are managed and also depending on the actions of other miners.

It can be shown that hoppers will earn more than normal ``continuous" miners.

Various reward and pool management methods have been proposed in order to discourage pool hopping and some reward methods can be shown to be immune to this attack.

[cf. Rosenfeld works]

Attacks:

- Mining Cartel Attack



Mining Cartel Attack

50% of miners decide to totally ignore blocks mined by other people. Likely to always succeed.

Only subversive miners make money from mining.

(there is no need to cheat on transactions, would also be possible for 50% of miners).

Attacks:

- Difficulty Raising Attack



*Difficulty Raising Attack

Very theoretical, powerful adversary.

[Lear Bahack 2013]

A powerful attacker is secretly preparing an alternative version of the blockchain.

At the same time he is manipulating the automatic difficulty adjustment mechanism in his secret chain in order to increase the probability of eventually that his chain will be recognized as surpassing the public honest chain.

If this happens, the attacker reveals his secret chain.

This can be used to commit double-spending or to cancel some transactions.

Confidential Crypto Optimisation Attack



Confidential Crypto Optimization Attack

A group of miners hire cryptologists to develop a secret method to mine more efficiently.

Similar but better than 39% gain of:

Nicolas Courtois, Marek Grajek, Rahul Naik:

The Unreasonable Fundamental Incertitudes Behind Bitcoin Mining, <http://arxiv.org/abs/1310.7935>

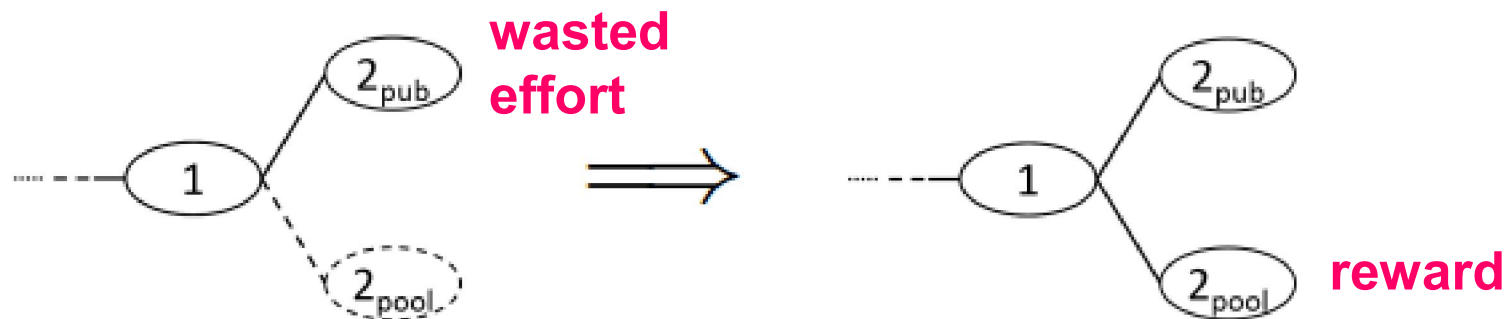
Selfish Mining and Block Discarding Attacks [2013]



Selfish Mining Attacks

Proposed independently by Eyal-Sirer [Cornell]
and also by Bahack [Open Univ. of Israel] in 2013.

It is about building secret extensions and disclosing them later.

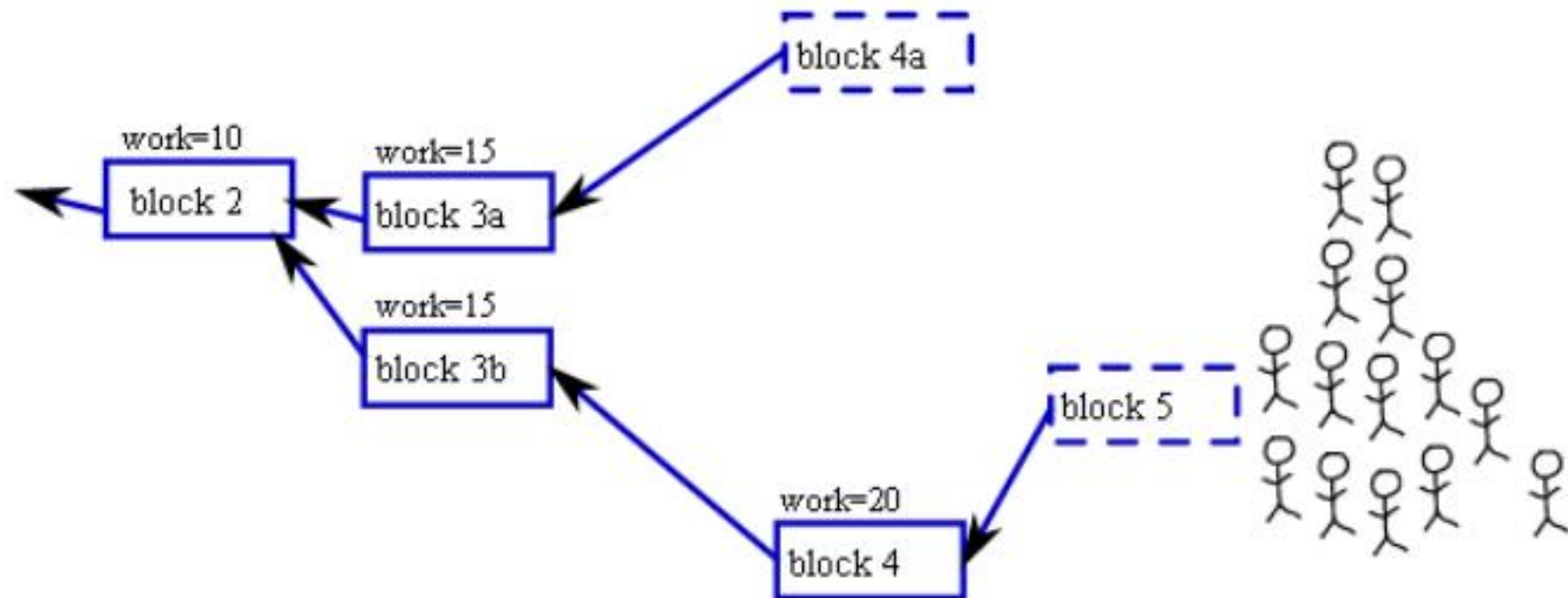


- In fact this is a very theoretical attack, most probably without a lot of practical importance...
- It relies entirely on “very rare events”,
 - most of the time there is no advantage to the attacker.

Selfish Mining Attacks

Assumption 1:

If there is the longest chain in the bitcoin blockchain,
everybody mines on it. Called “consensus”
Doing otherwise would be really stupid.

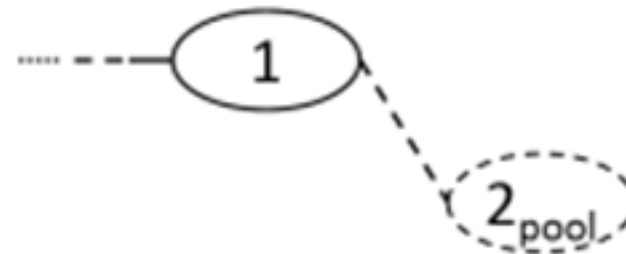


Selfish Mining Attacks

Assumption 2:

At any moment during the attack there are up to two competitive public branches one of which can have a secret extension.

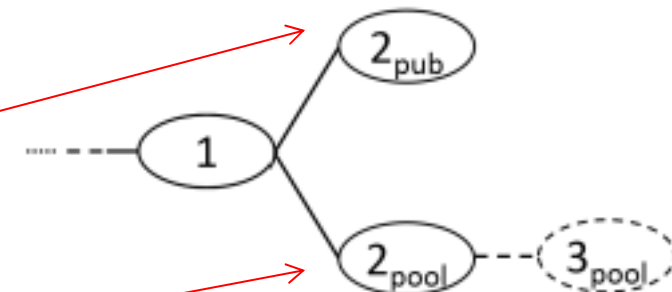
- we have either just one branch (with possibly a secret extension by the attacker's)



- or a public fork with two branches of equal depth k

in the case of a fork one branch is composed solely of honest miner's blocks

and the other is composed solely of attacker's blocks (which at moments can have a secret extension).

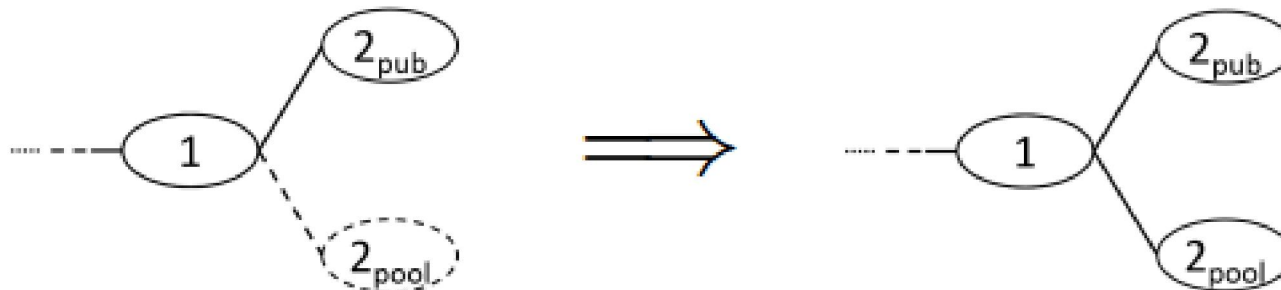


Selective Disclosure

Attackers keep their blocks secret for some time, in order to make the honest majority lose energy mining on obsolete blocks.

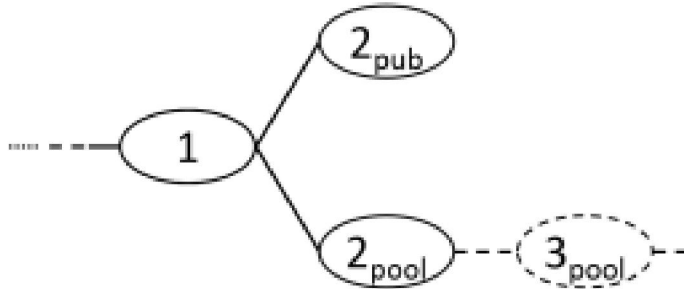


However when other find a block, subversive miners disclose their ASAP. Known to them A BIT earlier. Small advantage.



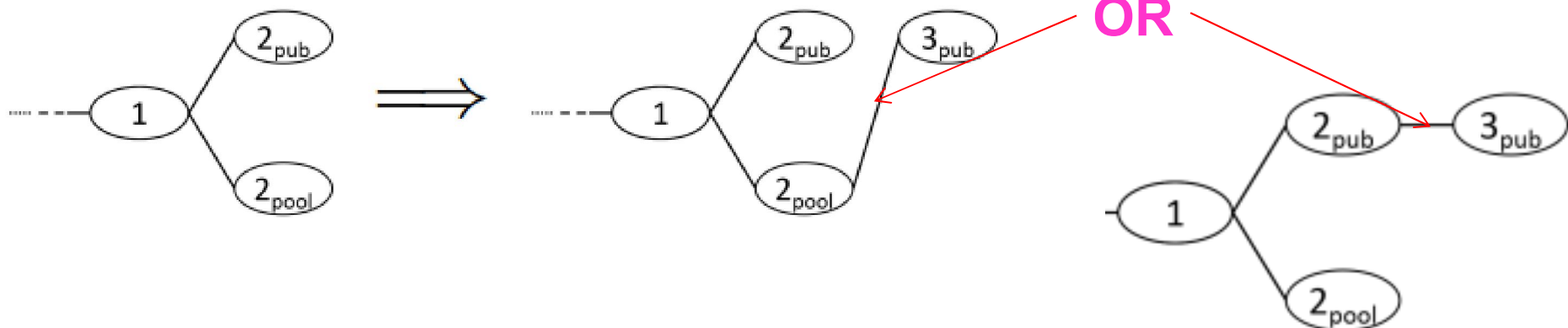
Fork Strategies

Subversive Miners mine on their own branch only.



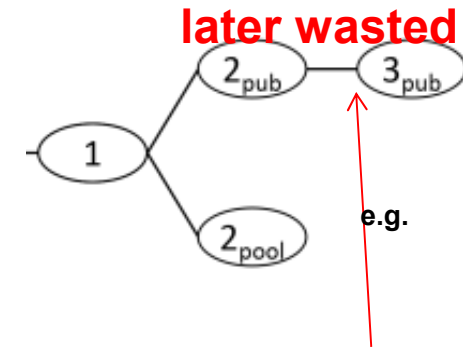
Honest miners mine on both, depending on network propagation[current state].

- received first [current bitcoin software]
- or chosen at random [suggested countermeasure]



Overall Result

Subversive miners can earn a bit more.
Not a big deal.



Remark[Courtois]
this attack is all about
events which almost
never happen
in the current
bitcoin network.

Unlikely to get
very significant...

blocks	<i>wasted</i>	<i>child(wasted)</i>
less than 140,000	0.00%	0.00%
140,000-149,999	0.21%	0.00%
150,000-159,999	0.27%	0.01%
160,000-169,999	1.01%	0.01%
170,000-179,999	1.77%	0.29%
180,000-189,999	1.71%	0.01%
190,000-199,999	1.15%	0.01%
200,000-209,999	0.88%	0.00%
210,000-219,999	1.05%	0.00%
220,000-229,999	1.28%	0.42%
230,000-239,999	0.78%	0.00%
240,000-249,999	0.43%	0.00%
250,000-259,999	0.67%	0.01%
260,000-now	0.91%	0.01%

Fix It?

Countermeasure 1: [Cornell researchers]

There is no minority attack if honest miners mine at random.

Countermeasure 2: [Bahack]:

Fork punishment [for all miners].

Will make the attack completely insignificant...

Our New Paper [2014]



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

Main Result

We revisit a known idea: block withholding.

The miners mine in pools, they report shares but in (very rare) case when they find the 'winning' tickets.

We show that this attack cannot be detected, not even in theory.

We show that for very large pools, it will be visible, but nobody can say who is responsible.

This attack was known [Rosenfeld] and in the initial version the subversive miners gained nothing: everybody lost.

Our Block Withholding Attack

We propose a better version,
in which subversive miners DO get more than their fair share.

It is very simple:

- 50 % of subversive miners withhold blocks they find
- 50 % mine solo normally (or in other pools).

We show that: 50-50 split maximizes the gain.

We claim that this simple attack is by far more practical and more realistic than the Cornell attack [1000s of press reports].

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>

Breaking News!

13 June 2014

a large-scale block-withholding attack

was executed against the mining pool Eligius

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

There is no proof it worked exactly as we say.

- Losses are very substantial and were estimated to be about 300 BTC - at the expense of honest miners (apparently).
 - This is 186,000 USD at recent prices

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.uc9l6ink.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].

Further Events

Eligius pool managers have contacted the “rogue” miners.

They have made public their bitcoin addresses:

17JkL94B2ngJg4QQZuiozDQjnxXB6B7yTc and

1Gu8zxRi8cyENV8CQe52D7QEsiZ7ruT73u

Would they use many addresses with smaller payouts, the attack would probably have been detected (see my slides/paper about standard deviation).

Rogue Miners

17JkL94B2ngJg4QQZuiozDQjnxXB6B7yTc

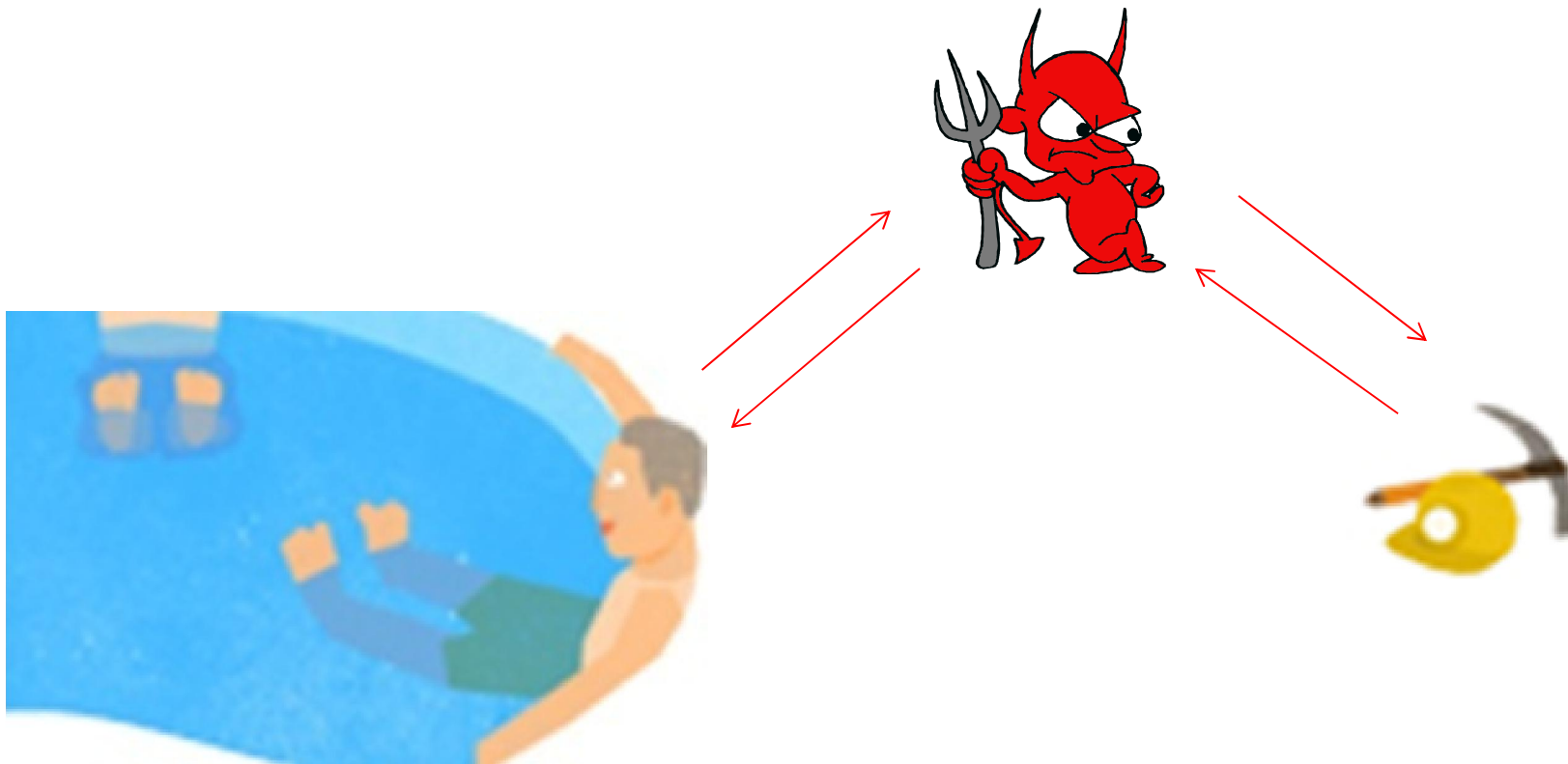
1Gu8zxRi8cyENV8CQe52D7QEsiZ7ruT73u

Eligius pool managers have blocked assets worth 200 BTC belonging to the attackers (balances not yet paid, due to a delay).

=> Considered stolen property belonging to the other miners.

- The attackers have threatened putting a 200 BTC bounty on hacking Eligius.
- more recently, their behaviors have extended to additional ultimatums,
- arbitrary deadlines,
- demanding 1164% interest on the payout ,
- etc .

MITM Attacks?

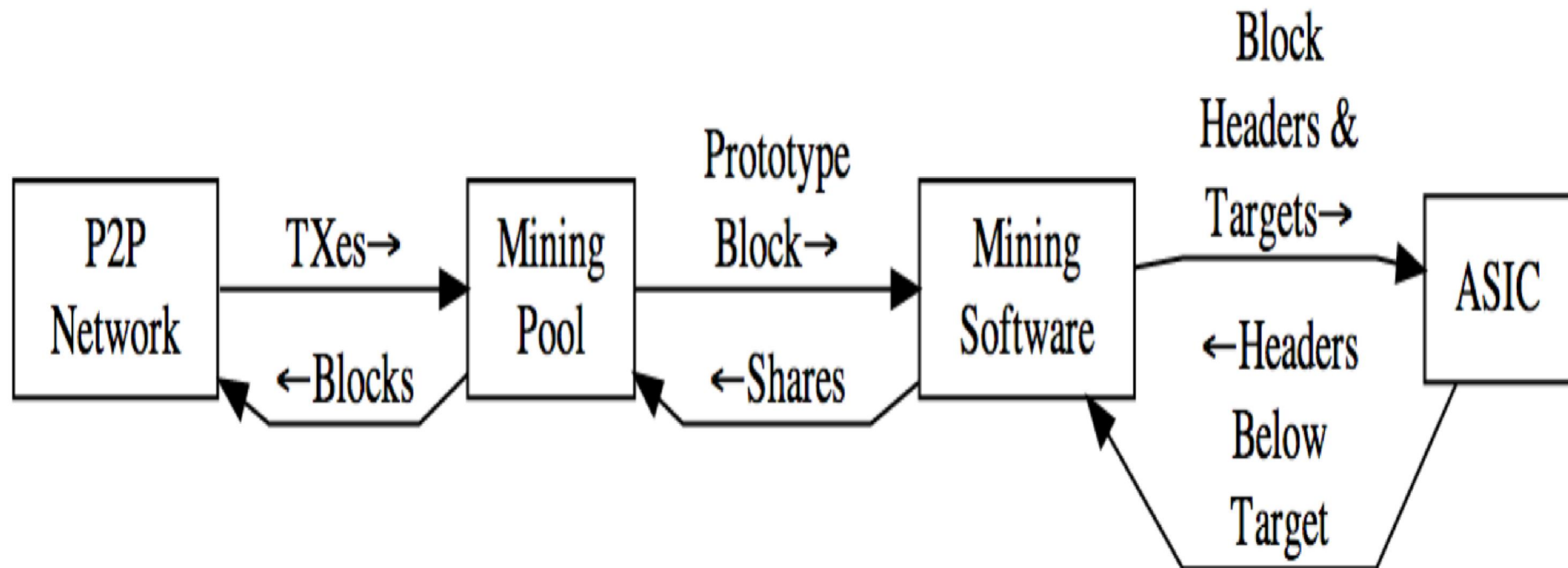


Possible Goals

- abuse miners
- steal the money (harder)

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

Stratum Protocol



Stratum

Protocol developed since Dec. 2011 as a 'layer above' the BTC network.

- Like super-nodes doing super work.
- Some bitcoin-related services.

For example:

- Distribution of metadata which are NOT recorded in the blockchain:
 - for example: signed messages about seeing something: against 51% attacks...
- Queries from trusted nodes by "light nodes",
 - like ask about transactions for a list of addresses etc.
- Possibly supporting alt coins or alt-chains... lots of possibilities.

Messages are formatted as plain text JSON-RPC (Remote Procedure Call).

- a line-based protocol using plain TCP sockets
- payload id encoded as JSON-RPC messages

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

Future: "I already have some ideas for Stratum mining protocol extension, where miners will be able to suggest their own merkle branch (I call it internally "democratic mining"), which will solve such issues as centralized selection of transactions. For now I decided to focus on such a solution, which will fit to majority of miners and do some extensions later.

Previous solution was: "getblocktemplate over HTTP", it did allow miners to choose... did not scale up well.

A Birth of a Cartel

A tiny bit earlier, the bitcoin open community has developed a superior* decentralized solution
GBT (GetBlockTemplate) or BIP 22/23

<https://en.bitcoin.it/wiki/Getblocktemplate>

*well actually slush claimed that Stratum is more practical in all aspects except... on centralisation
see Section “Stratum versus getblocktemplate” in <https://mining.bitcoin.cz/stratum-mining>

Stratum was backed by a major mining pool and GBT adoption suffered.

⇒ a **cartel** of two sorts of super highly centralized entities has emerged:

- designers of mining ASICs and people who run pool managers.

These people together were able to impose a protocol which represents their interest, and which makes centralization possible, possibly forever.

- a sort of hold-up: bitcoin became **maybe irreversibly centralized** by adopting a protocol which shifts the power to pool managers
- irreversible unless miners revolt!

JSON-RPC

RPC=Remote Procedure Call,

Example of JSON-RPC:

```
--> {"method": "echo", "params": ["Hello JSON-RPC"], "id": 1}  
<-- {"result": "Hello JSON-RPC", "error": null, "id": 1}
```

Stratum in Pooled Mining [Most Pools]

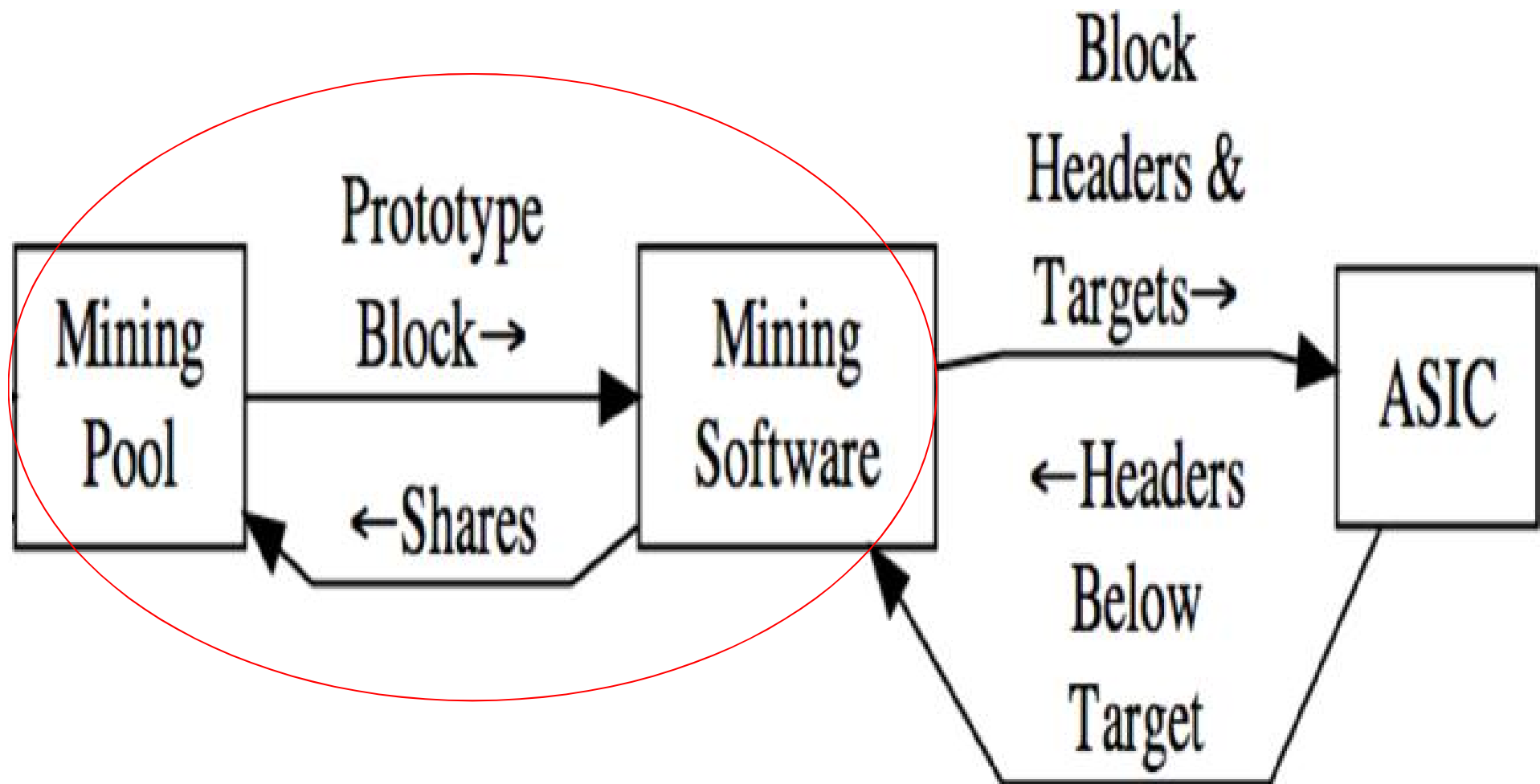
Pushing work:

- Work is sent to miners.
- They can carry on for a very long time, without contacting the server.
 - they send shares with an asynchronous socket, not opening/closing HTTP connections.
- At one moment the work suddenly becomes obsolete,
 - the server notifies immediately and sends new work.

Miner side:

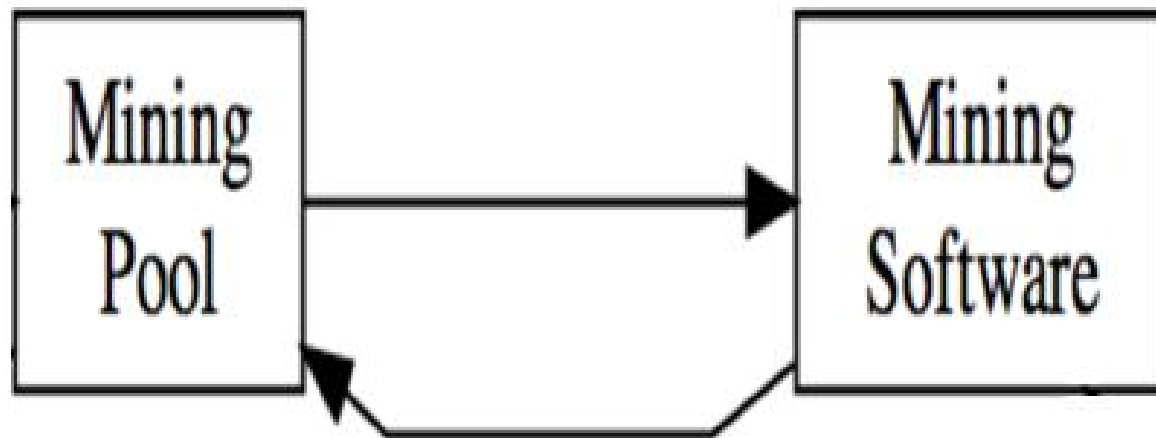
- Every 2^{32} steps or so miners increment a counter in the coinbase transaction (they run out of nonces, there is also certain flexibility in `nTime=current timestamp in seconds`).
- They are also allowed???? To build a new Merkle root adding latest transactions???

Overview



Stratum Stages

1. Subscription/connection
2. Authorize a worker
3. Server work => worker
4. Shares <= server



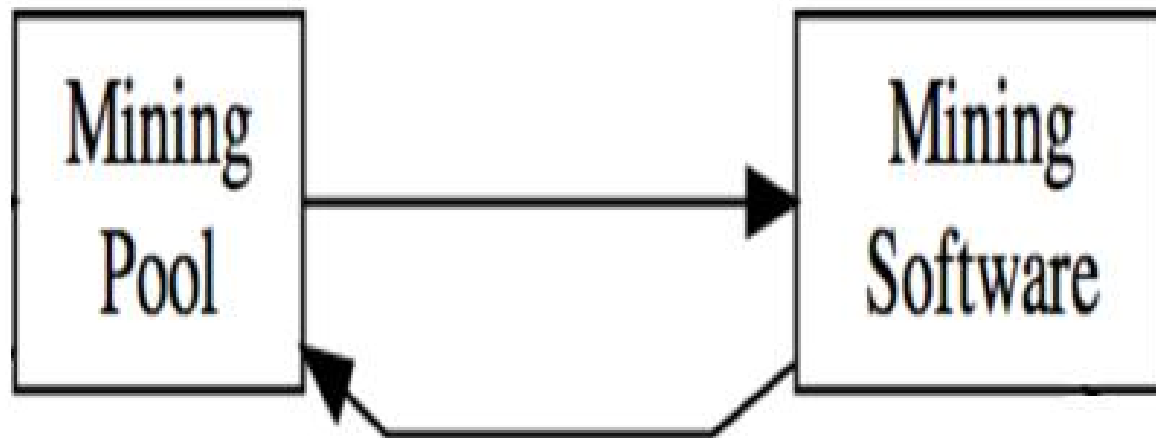
Subscribe

Server

Worker

=> **ExtraNonce1**

1. Subscription/connection
2. Authorize a worker
3. Server work => worker
4. Shares <= server

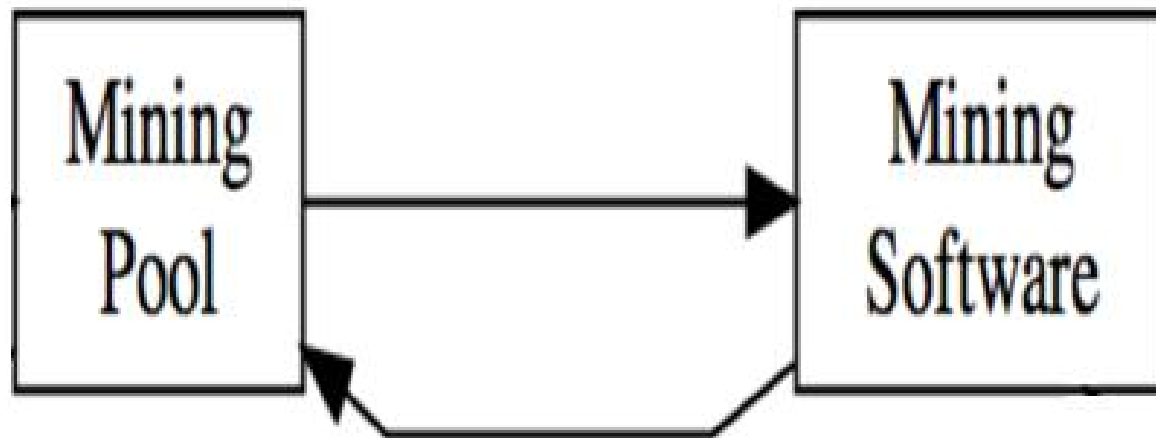


Real-Life Subscribe Example [Eligius]

```
<= {"id": 3011861, "method": "mining.subscribe", "params":  
["cgminer/3.8.1", "9036b6080000000001"]}  
=> {"result": [[["mining.notify", "d0e079100000000001"],  
["mining.set_difficulty", "d0e079100000000002"]], "d0e0791000000000", 4],  
"id": 3011861, "error": null}
```

ExtraNonce1

size(ExtraNonce2)

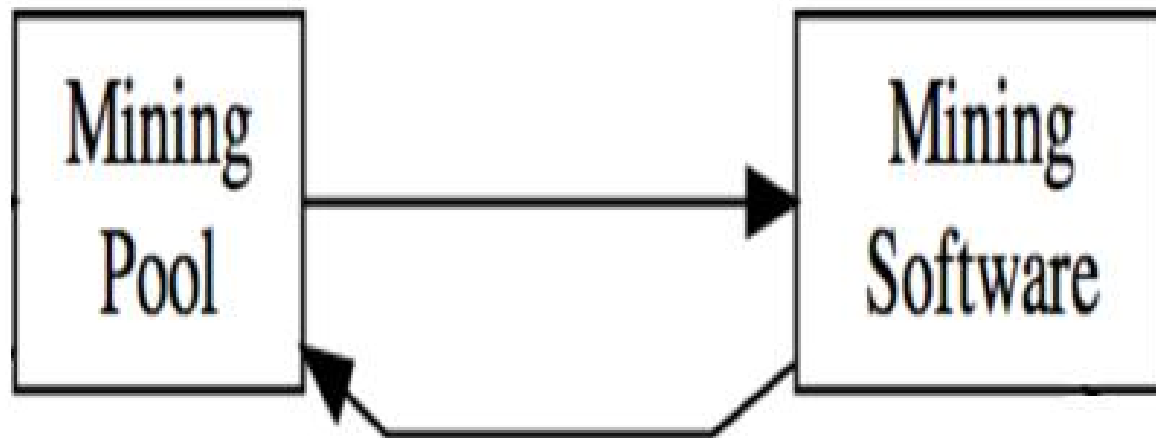


Real-Life Subscribe Example [DiscusFish]

```
<=      {"id": 242, "method": "mining.subscribe", "params":  
["cgminer/3.8.1", "f66bee79"]}  
=>      {"id":242,"result":[[["mining.notify","60999f56"],  
["mining.set_difficulty","mining.set_difficulty"]],"60999f56",4],"error":null}
```

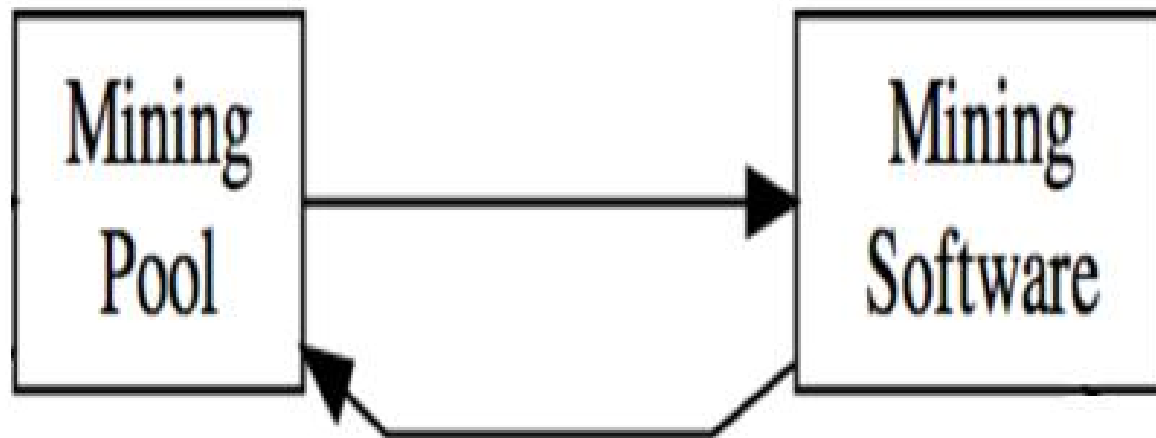
ExtraNonce1

size(ExtraNonce2)



Another Example Found

```
<= {"id": 1 "method": "mining.subscribe", "params": []}  
=> {"id": 1, "result": [[["mining.set_difficulty",  
"b4b6693b72a50c7116db18d6497cac52"], ["mining.notify",  
"ae6812eb4cd7735a302a8a9dd95cf71f"]], "08000002", 4], "error": null}
```



are these 2 hard-coded constants?

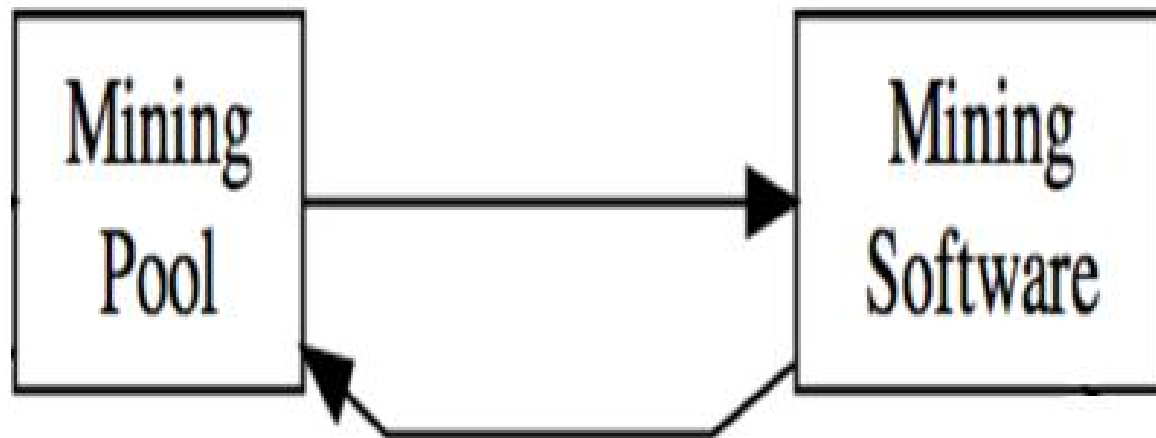
<https://github.com/Stratohm/stratum-proxy/blob/master/src/main/java/strat/mining/stratum/proxy/worker/StratumWorkerConnection.java>

Details

```
<=      {"id": 1 "method": "mining.subscribe", "params": []}  
=>      {"id": 1, "result": [[["mining.set_difficulty",  
"b4b6693b72a50c7116db18d6497cac52"], ["mining.notify",  
"ae6812eb4cd7735a302a8a9dd95cf71f"]], "08000002", 4], "error": null}
```

ExtraNonce1

size(ExtraNonce2)



Authorize – Just After Subscribe

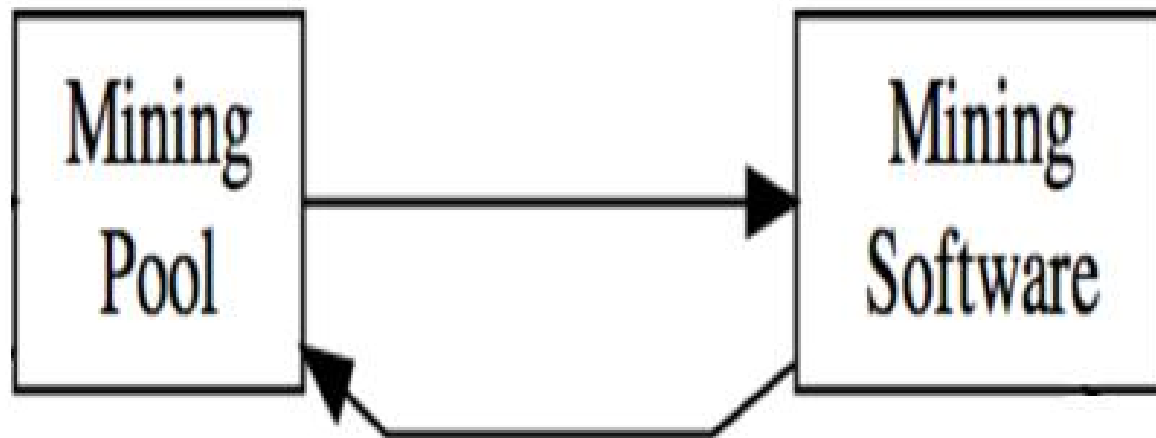
Server

Worker

=> **ExtraNonce1**

Miner Name <=

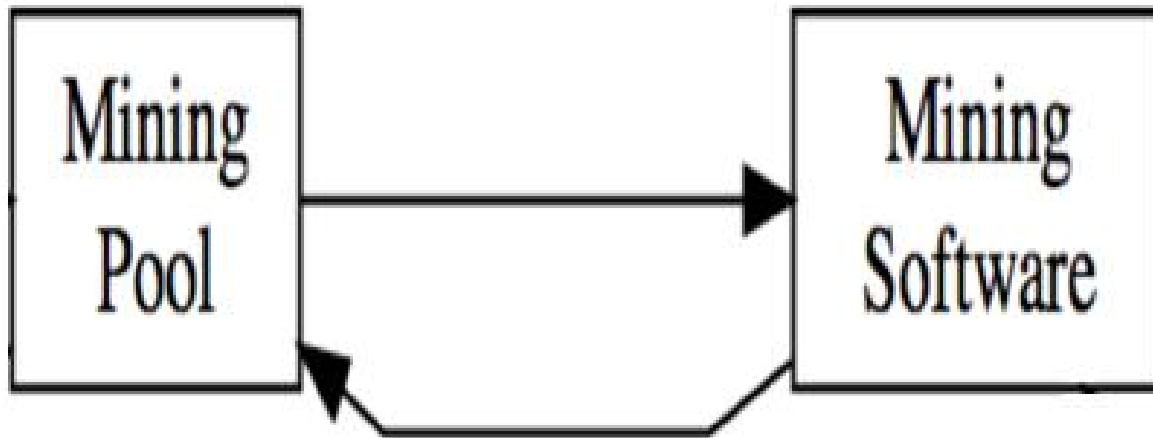
1. Subscription/connection
2. Authorize a worker
3. Server work => worker
4. Shares <= server



Authorize Details

```
=> {"params": ["miner_name", "password"],  
      "id": 2, "method": "mining.authorize"}
```

```
<= {"result": true, "id": 2, "error": null}
```

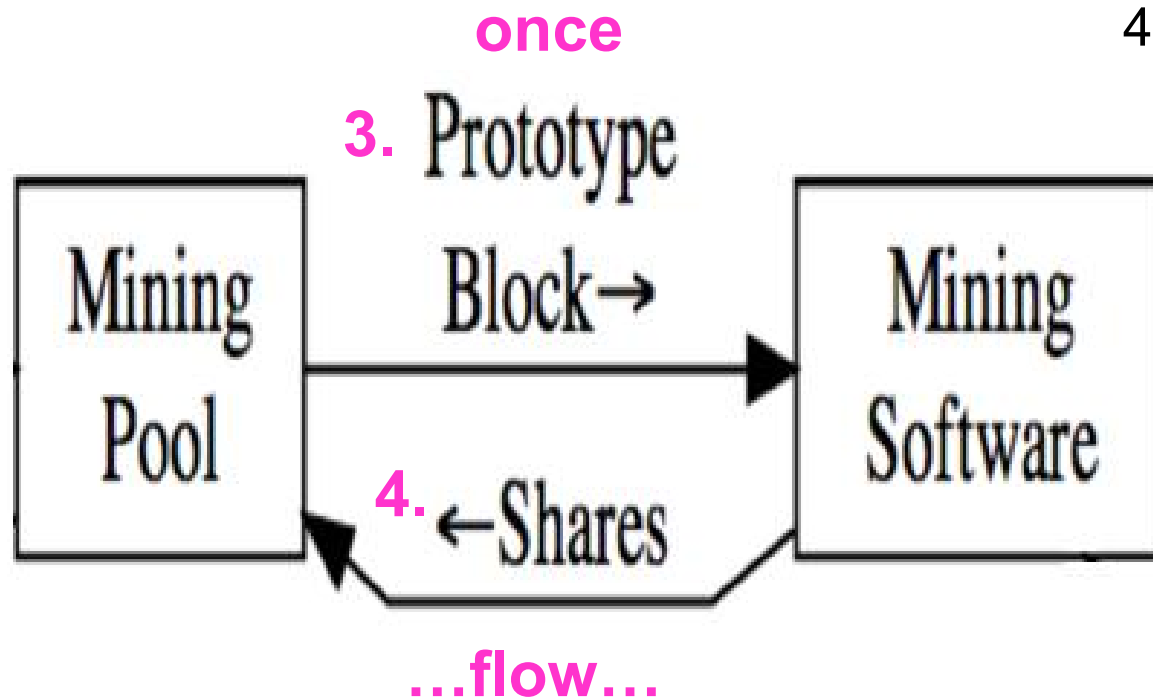


3-4. Mine!

Server

Worker

1. Subscription/connection
2. Authorize a worker
3. Server work => worker
4. Shares <= server



3. Server Work Communication (mining job)

(Eligius)

```
Server: {"params": ["1403009309 11666",
"292ad15f13fed14a9a1316b9f52b9d3a234a2f572ab8bd210000000000000000",
"0100000001000000000000000000000000000000000000000000000000000000ffff",
ffff52038bac040d00456c69676975730053a0391dfabe6d6d245d64a852df57ba3cf5c24b53e459a",
b9dba49e37f724a70637956ee3754d3ce0400000000000000002f737332332f00",
"ffffffff1a180440000000000001976a9143810f95cc7d5d9b06c378244172aa8311681f1a488ac568",
9400000000000001976a91460876095942498c23f4071d615db8982550d60f788ac2c994000000000",
001976a9144ebf00154078a5ee78599adb4a82ce3b75709f5688acef0840000000000001976a91429",
...00001976a9148ec06cc970e54b5dfe10a90c1eff2232d2300d1b88ac1d074100000000001976a9",
14e40a50aef7f788ac81d14000000000001976a914e078ecbed20e721047e5e2603886c5ae4f5ffac",
788ac6667ae83000000001976a914ecf0dfe07072afaed4135e99c70072cce2235a7f88ac01000000",
000000001976a9145399c3093d31e4b0af4be1215d59b857b861ad5d88ac00000000",
["68d4a3ad27c5d28db7822fec92e7cac4df87fe5ac10da74b1d52e01c7da4ce6a",
"56915e09578a0de92d75ba99cf62a8efc349522aeb22a3666c7bfda46a4d1d1d",
"c2f5fb89e3c57661e24dca08e9c7136ecfccaefcf0f05dc835c04a3fa0d844d",
"030caee1ca788183fff3a36ace4bb349d8c2b3ed8179a8645cb6c5123a2517bb",
"cf21863105d786b879fd4f8dcadac718b4463c92eb6c146babf8bdc1a9ac2df8",
"cf4f6d1fd9eff04c195c60bbd313361249e78615d3ca4e8aa429450aa5fa597a4",
"cf30725051d4ea58b092e96296021393fcc3d3706b597b9eb58866fc994f40f0",
"8b8684e57f660235abe876ec5d1ed349d52f9b8cffa9588eb1327f8e00f4a2cd"], "00000002",
"185d859a", "53a0391d", false], "id": null, "method": "mining.notify"}
```

– timestamp

– prevhash
makes the attacks detectable

– coinbase1

– coinbase2

– merkle
8-11 observed
branches

– 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!
(Eligius pool)

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!**

4b. Building Coinbase Transaction =

- Coinbase1 + Extranonce1 + Extranonce2 (padded) + Coinbase2

Extranonce2 = 0,1,2, etc....

Typically on 4 bytes.

Each value allow the miner to check 2^{32} nonces.

4c. Building Merkle Root

The coinbase transaction is passed through a double SHA256 to get the a hash value.
Combine it with the first merkle branch, and double SHA256 the combined string.
Then take that result, and do the same thing with the next merkle branch,
repeating this process until all merkle branch hashes have been combined with previous results.
The final result is a unique merkle root for the block header.

Difficulty [can be frequently changed]

```
{"params": [511.9921875], "id": null, "method": "mining.set_difficulty"}
```

**=> Roughly speaking it is adjusted
so that we have one message every
1-30 seconds...**

Example:

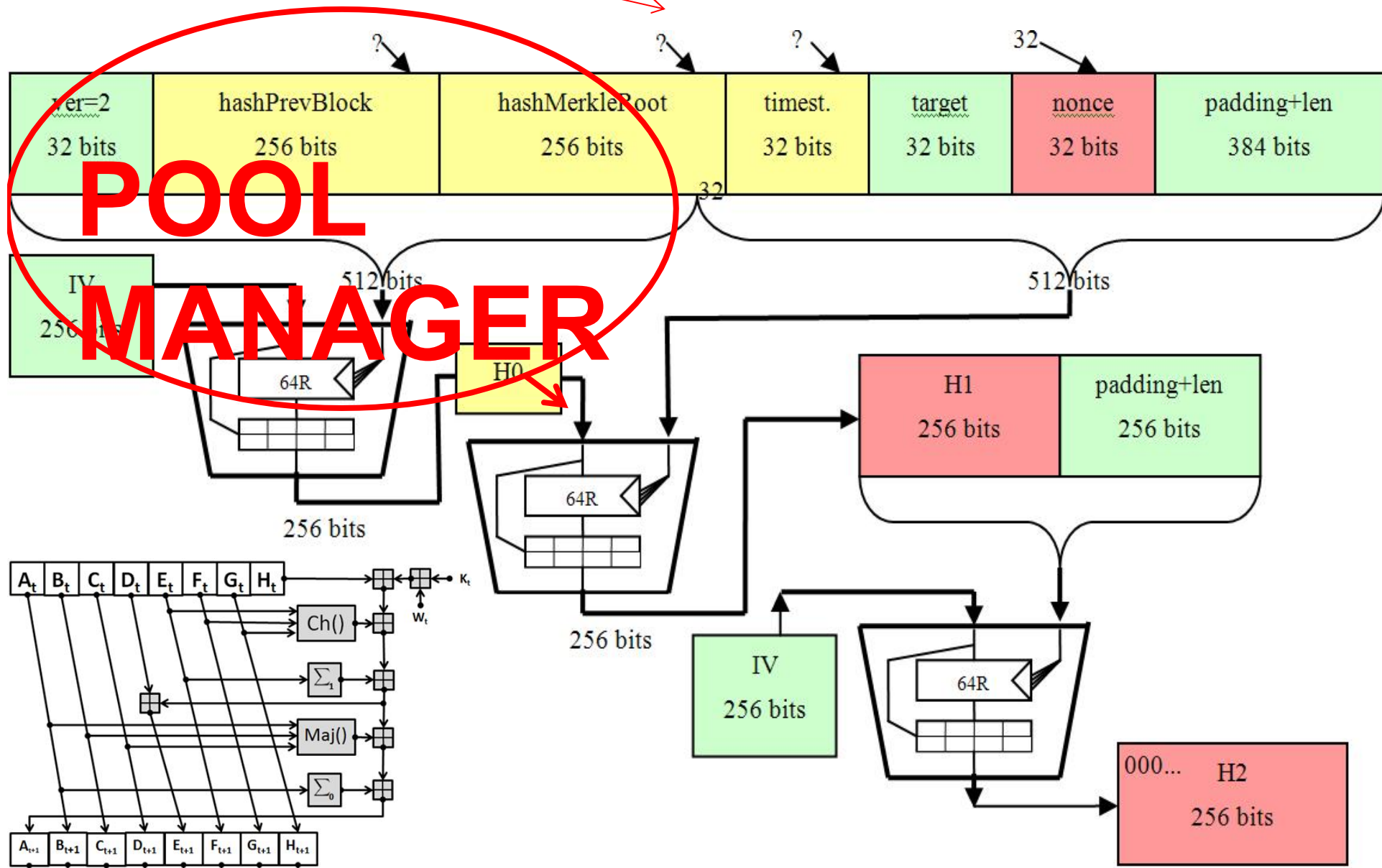
Time period	Shares submitted	Difficulty	Frequency
435s	158	512	0.36/s

$$\text{Hash rate} = \frac{\text{difficulty} * 2^{32}}{\text{time to find a share}}$$

$$\begin{aligned}\text{Hash rate} &= 512 * 2^{32} / (435\text{s} / 158 \text{ shares}) \\ &= 799 \text{ GH/s}\end{aligned}$$

hashed data from
previous transactions

***Scenario H0



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 clockchain 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.**

****Large Scale Attacks**



**Buying a Fork

A fork in the main chain
can be created retroactively...



- ⇒ In order to cheat: roll-back one or many large transactions from 0-4Y ago.
- ⇒ However high is the bitcoin price at any moment in the future, we have the following problem: in the future the percentage of newly created coins in 4 years (\geq the price of roll-back), is becoming increasingly small compared to all the existing money in circulation in the Bitcoin network...
- ⇒ So money at risk in BTC increases or stabilizes, cost to mine full 4 years in BTC does DECREASE every 4 years!