Bitcoin Mining and Improvements

Lublin, Poland 22 Sept 2014

Nicolas T. Courtois

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

Our Works on Bitcoin

- 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

⇒ **Section 2.6: Analysis of Bitcoin From The Point of View of Investors**

-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

Introducing Bitcoin

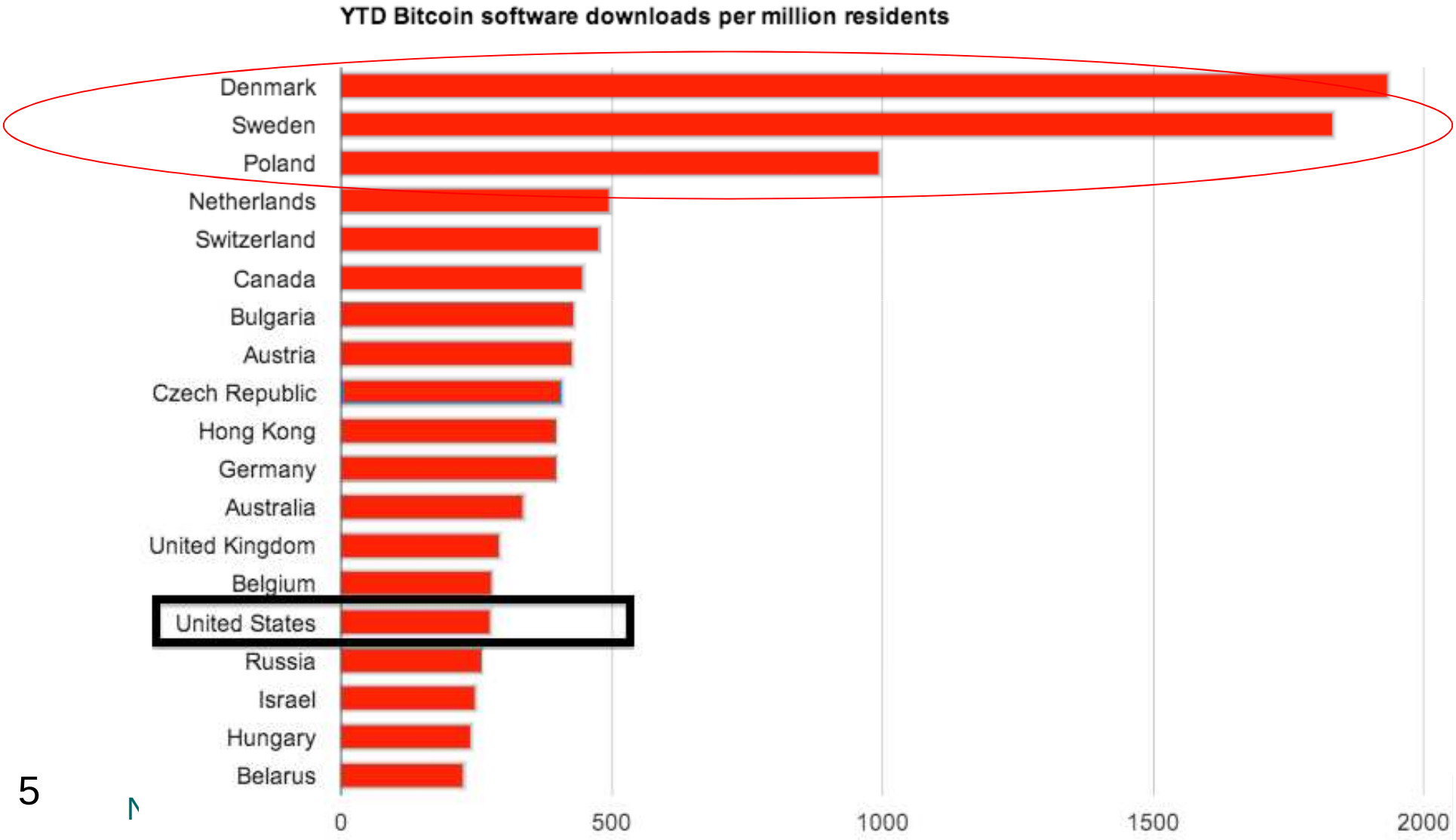
Bitcoin In A Nutshell

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

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

Poland = 3rd Place Worldwide

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



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:

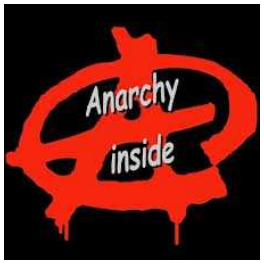
- "trust"

  => P2P self-regulation

  <= self-interest?

- legal/government protection and policing

  => anarchy!



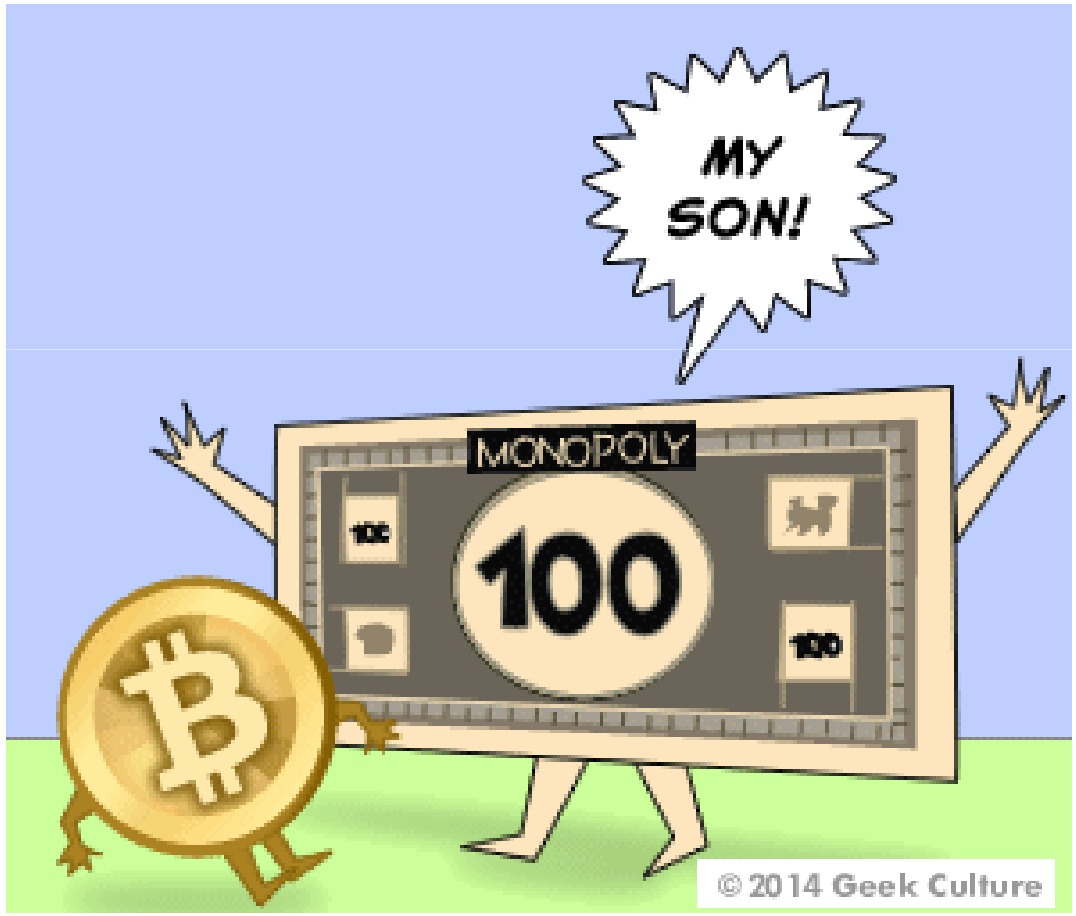
Citations

Bitcoin is:

- Wild West of our time [Anderson-Rosenberg]

Play Money?

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



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]

In Practice


11:00
KEYS
BALANCE
TRANSACTIONS
1Lke9VyQHixh
8zxteh7mENSr
4wsX5N6BeN
249.9 mBTC
~USD 184.43
Receiving 25 mBTC
Send
Receive
1 BTC ~ USD 738.00 (Bitstamp)

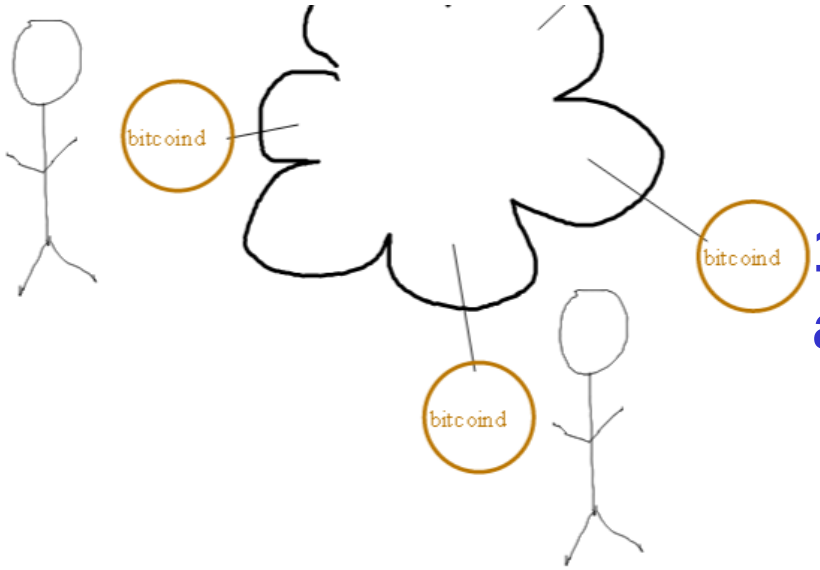
P2P Payment

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 Properties

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

– everybody participates equally

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
  - 100,000 people maybe
- some “full nodes”: they trust no one
  - 5,000 only
- wallet-only nodes
  - millions but not very active

*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

Digital Currency

Digital Currency

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

Main Problem:

This capability can be “spent twice”.

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

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

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

Crypto

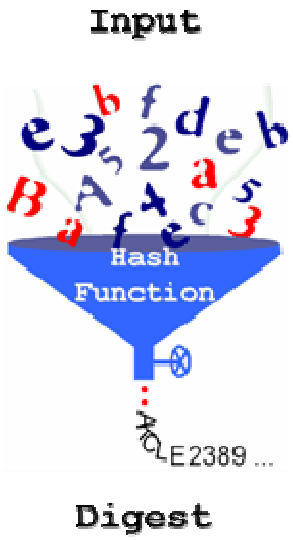
**Crypto Citations

About Bitcoin:

- The accuracy of past transactions is guaranteed by cryptography,

SHA256

- SHA-256 hash function
- provides integrity of everything [hard to modify]



Block Chain

Bitcoin Mining

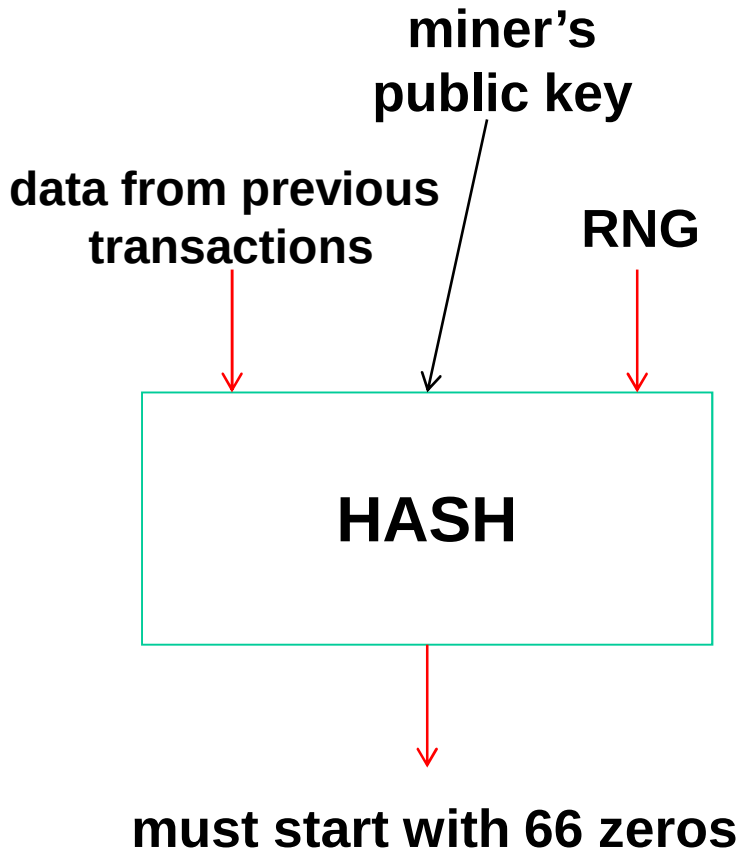
- Minting: creation of new currency.
- Confirmation+re-confirmation of older transactions

Random Oracle – like mechanism

Ownership:

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

[a part of] 25 BTC produced.



Block Chain

Def:

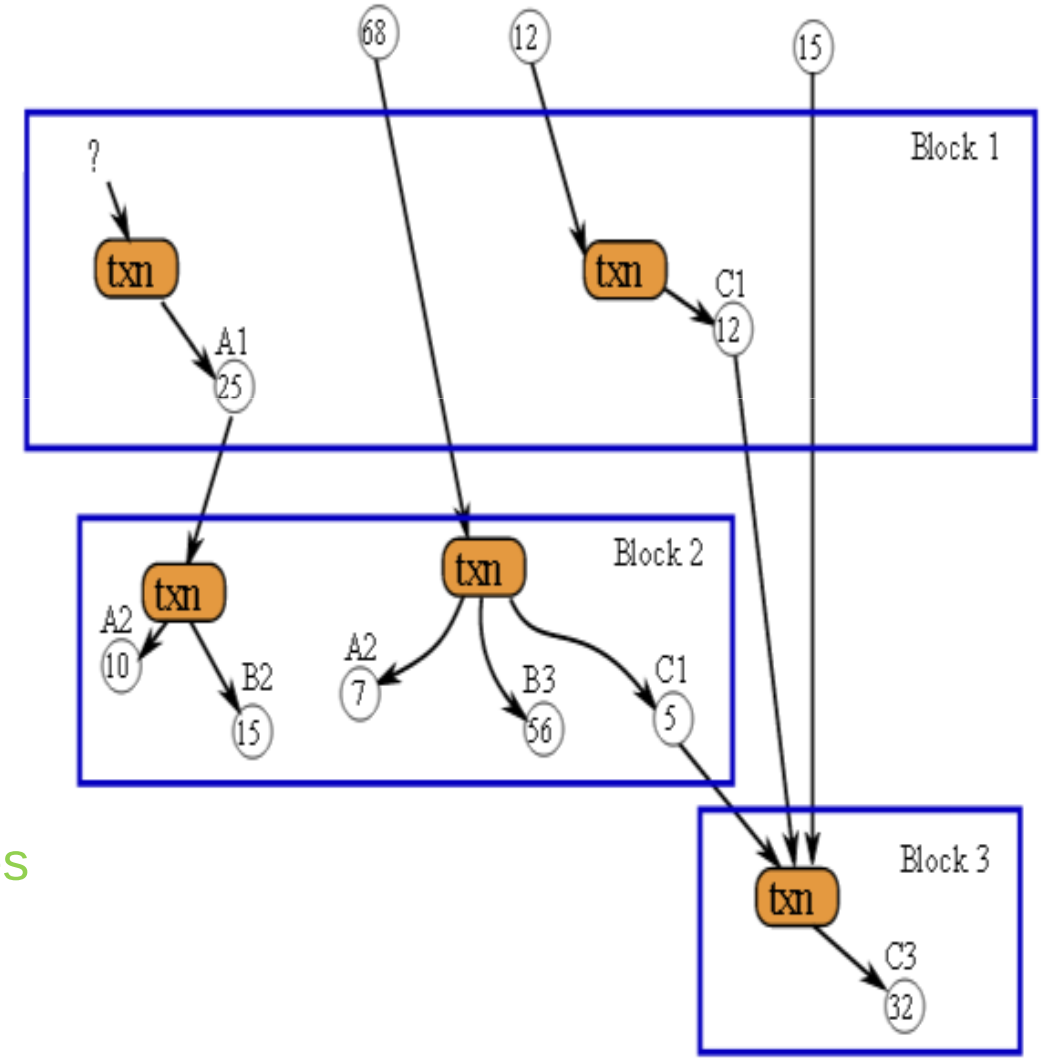
A transaction database shared by everyone.

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)

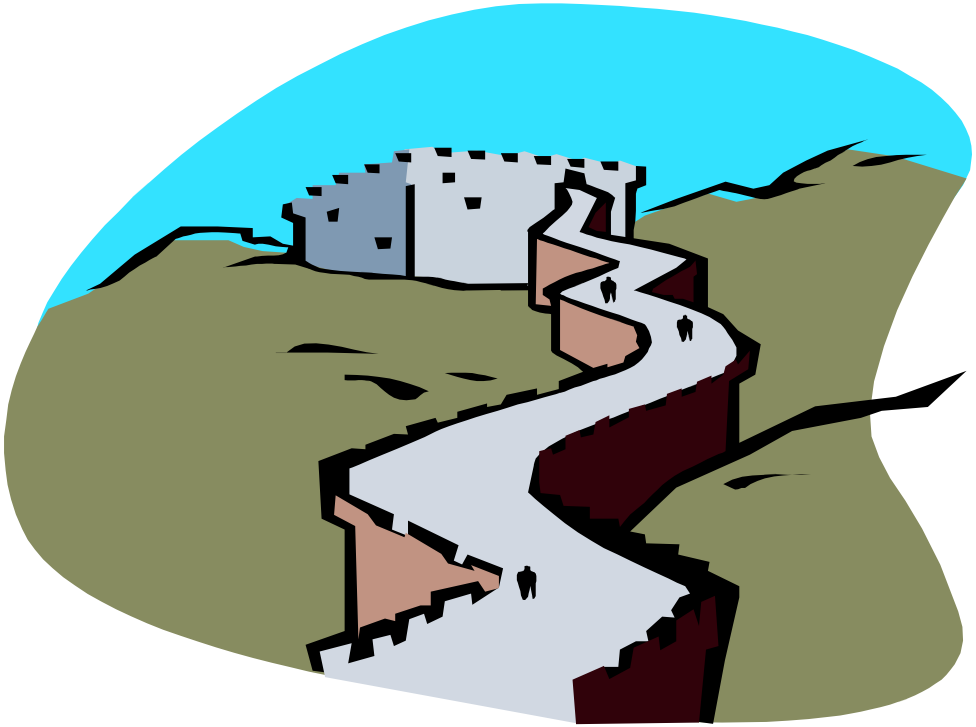


Hash Power => Security???

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 […]

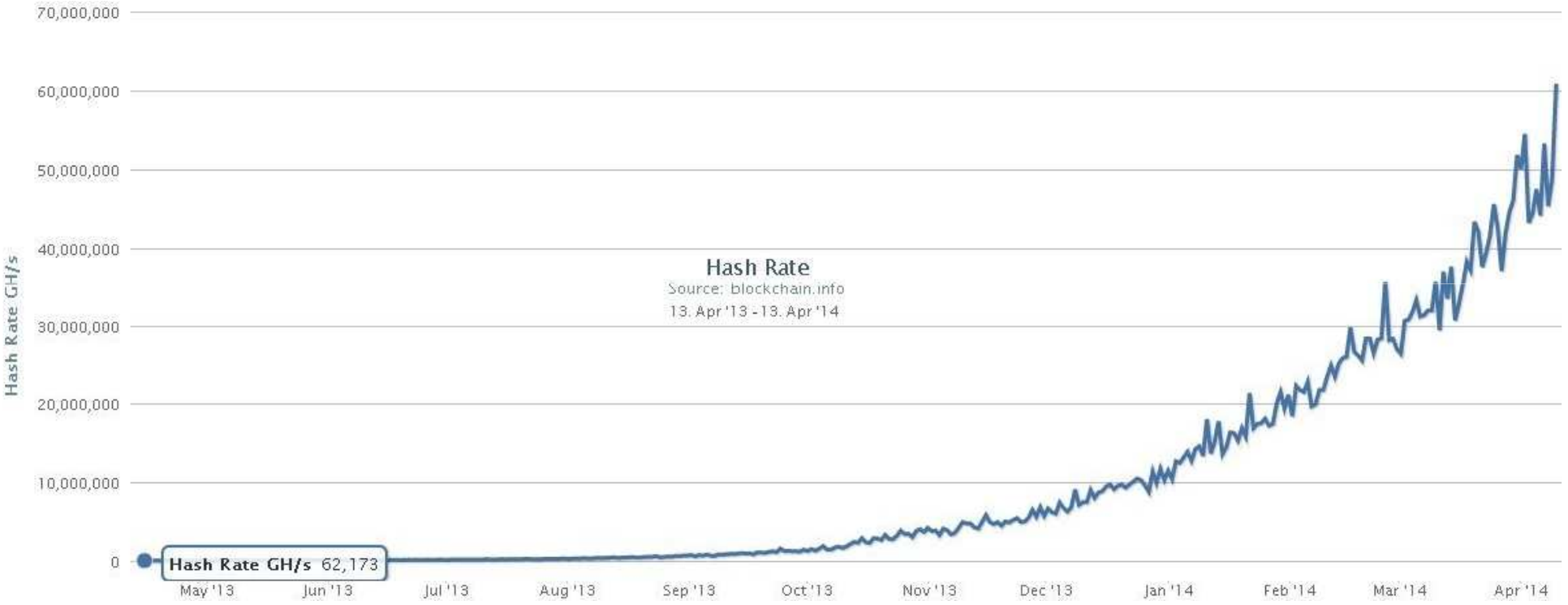
NO THIS IS MISTAKEN

(see our paper)



Crazy Hash Power Increase

Nearly doubled every month… 1000x in 1 year.



Thm:

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

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

Bitcoin Address

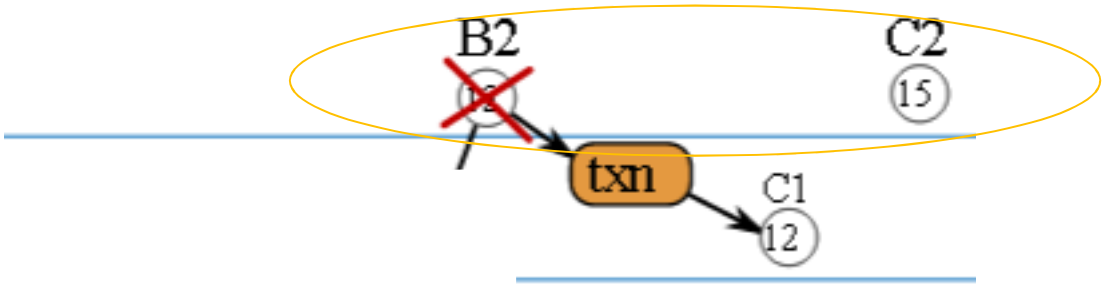
Ledger-Based Currency

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

Bitcoin Ownership

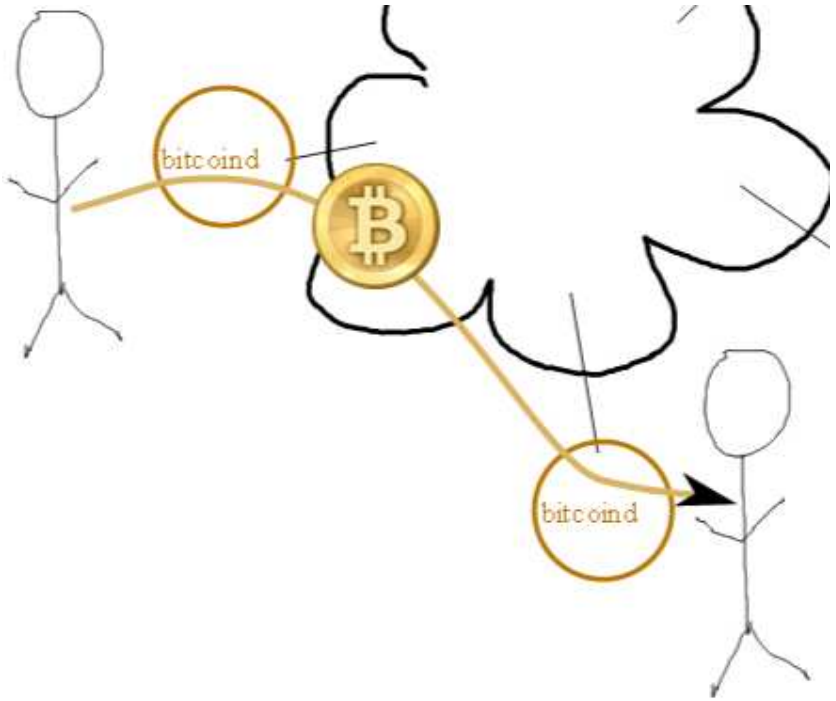
Amounts of money are attributed to public keys.

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



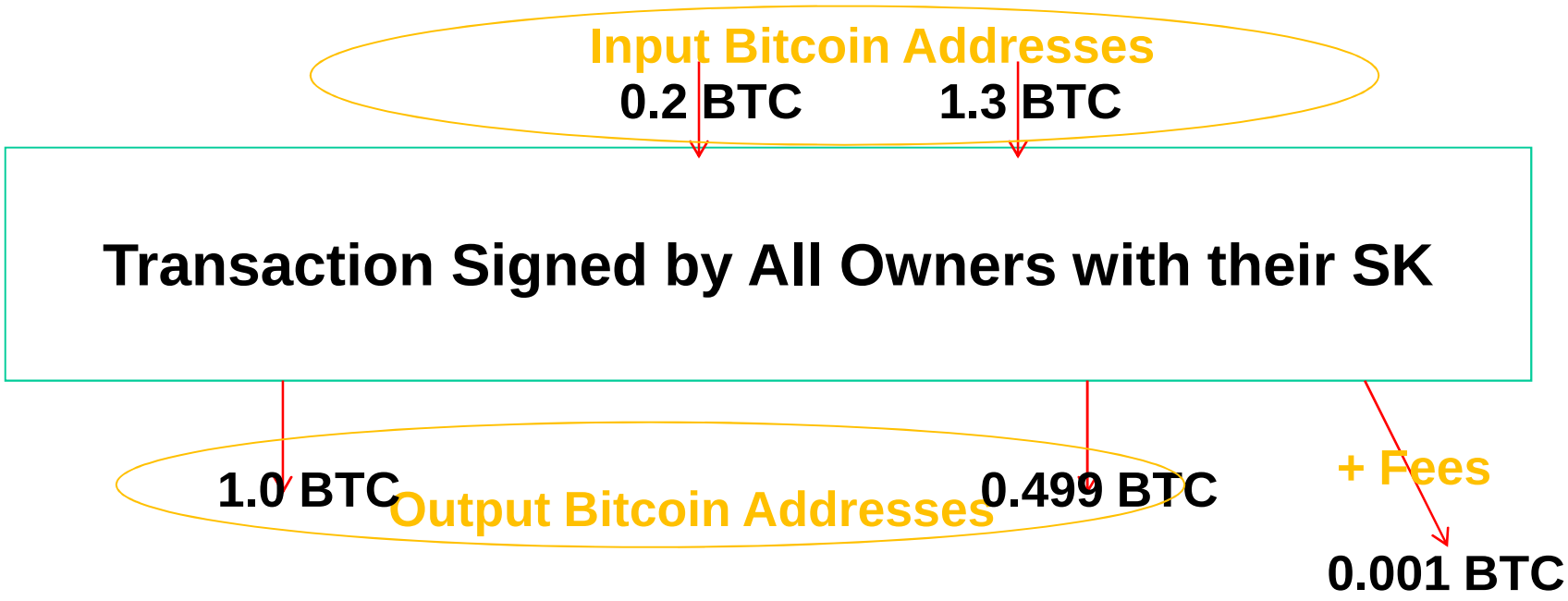
Transfer

To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36
Amount: 1.0 BTC
SEND



Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



Bitcoin Mining

Money Out of Thin Air

Bitcoin vs. Klondike

2012-2014

>100,000 miners

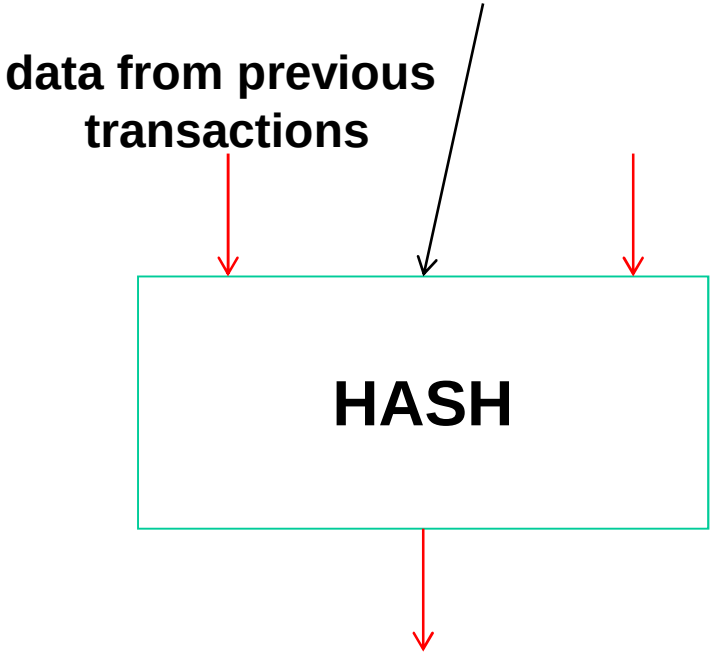
maybe ½ - ¾???? were victims of scams and paid for miners were not delivered in reasonable time

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

Bitcoin Mining

- Minting: creation of new currency.

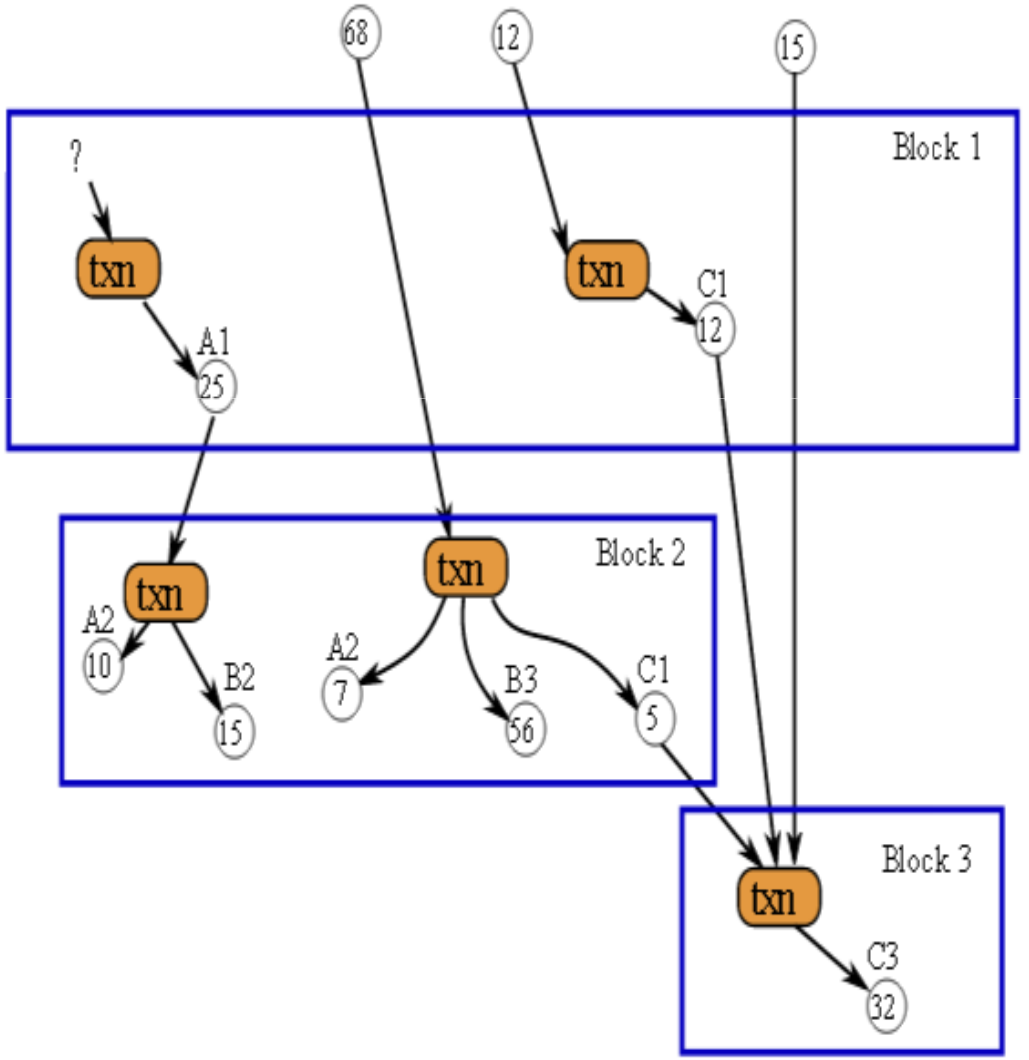
Creation of “money”
+re-confirmation
of older transactions



Block Chain

Def:

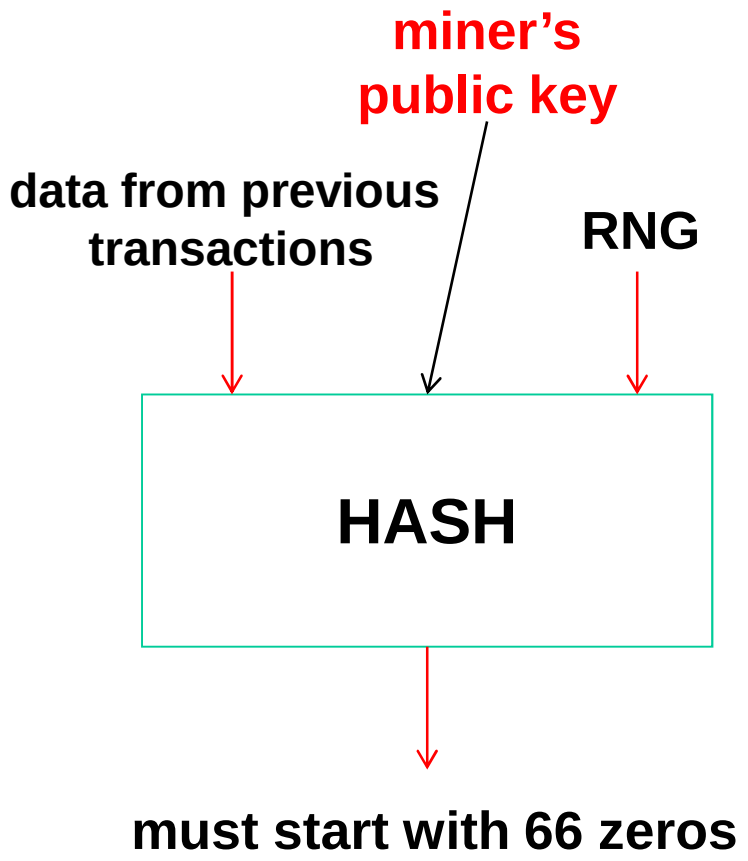
The bitcoin transaction database shared by everyone.



Bitcoin Ownership

Ownership:

- "policed by miners":



Bitcoin Mining

- Minting: creation of new currency.

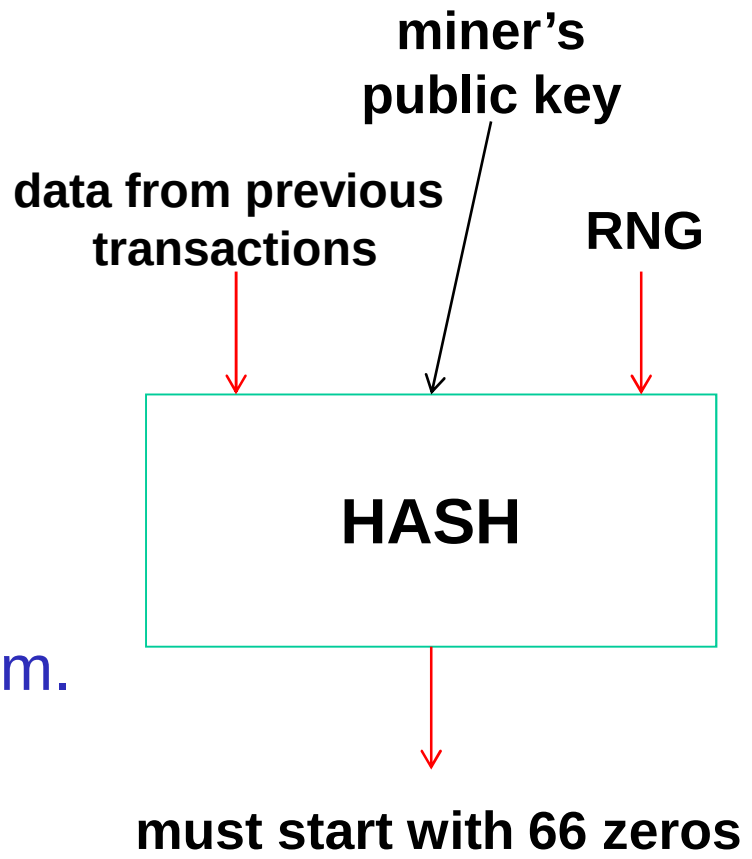
Creation+re-confirmation
of older transactions

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.



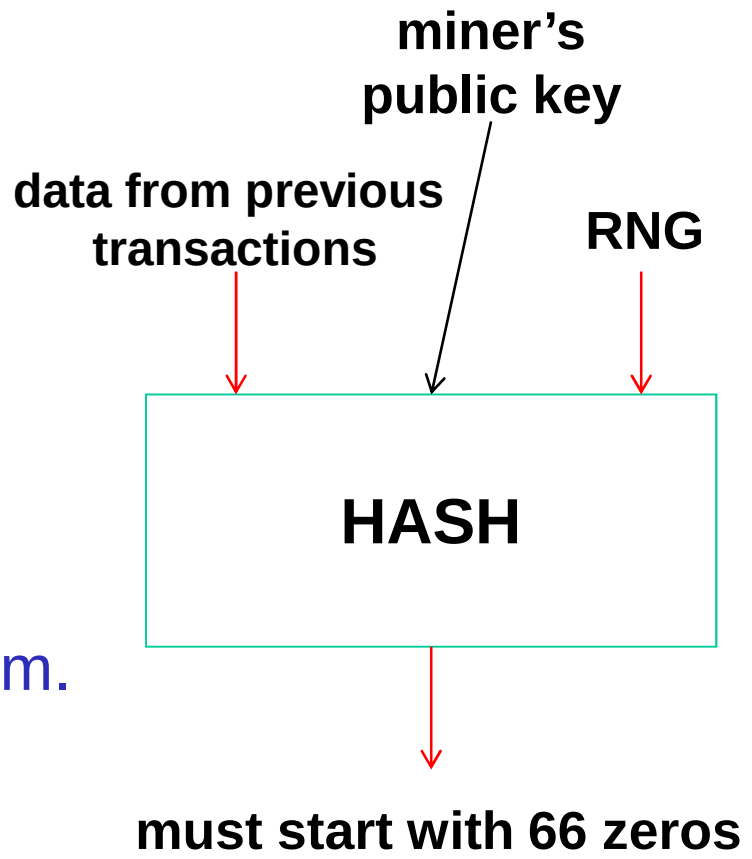
Bitcoin Mining

- 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

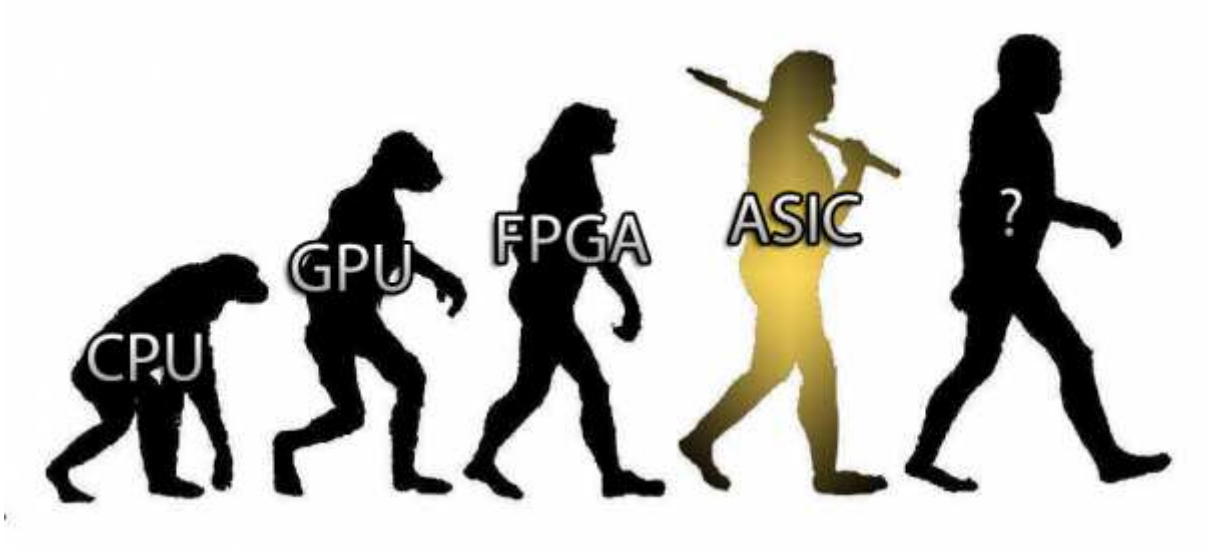
1. CPU Mining

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:

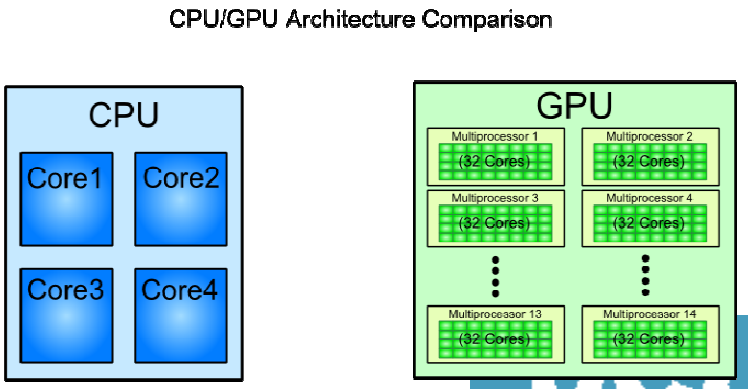
NVIDIA Quadro NVS 3100M, 16 cores, 3.6 Mh/s, 14W

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.



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

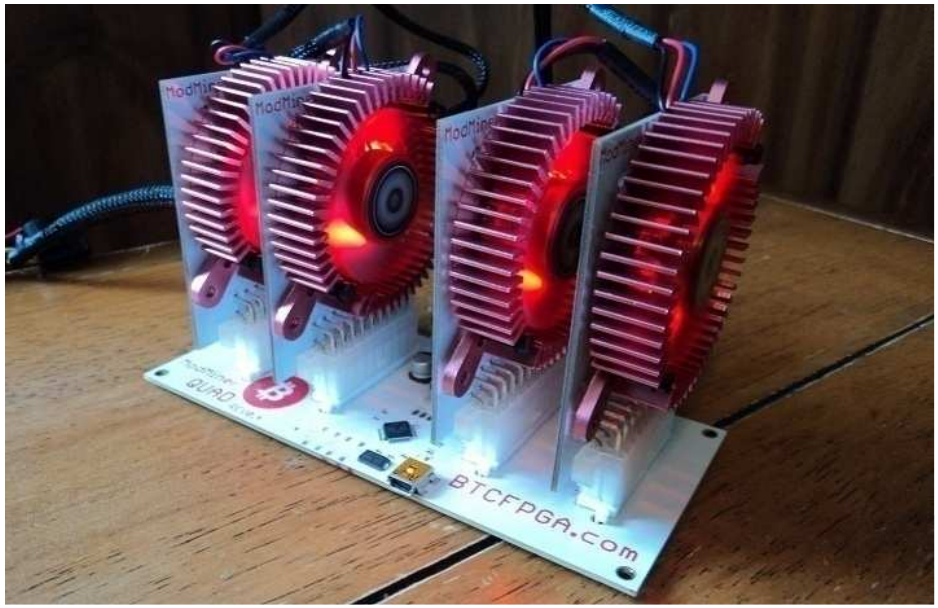
Example:

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

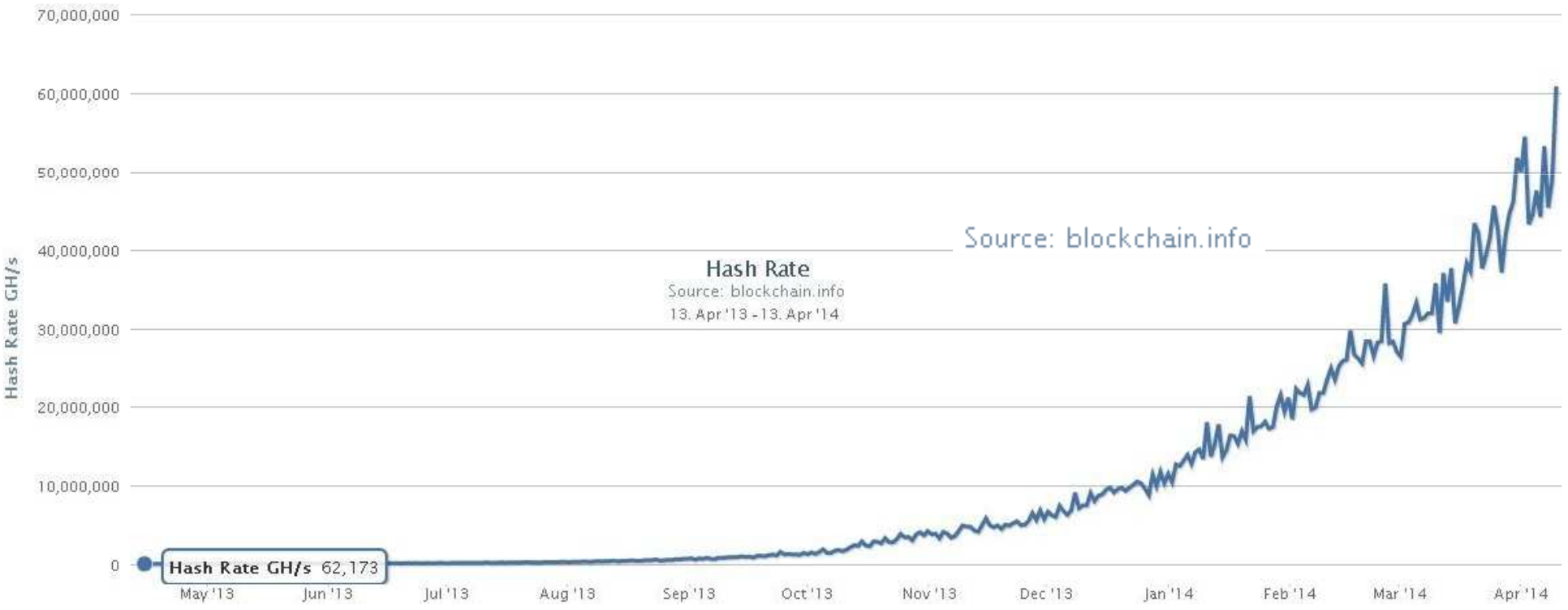
ASIC = now down to 0.35 W / Gh/s

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

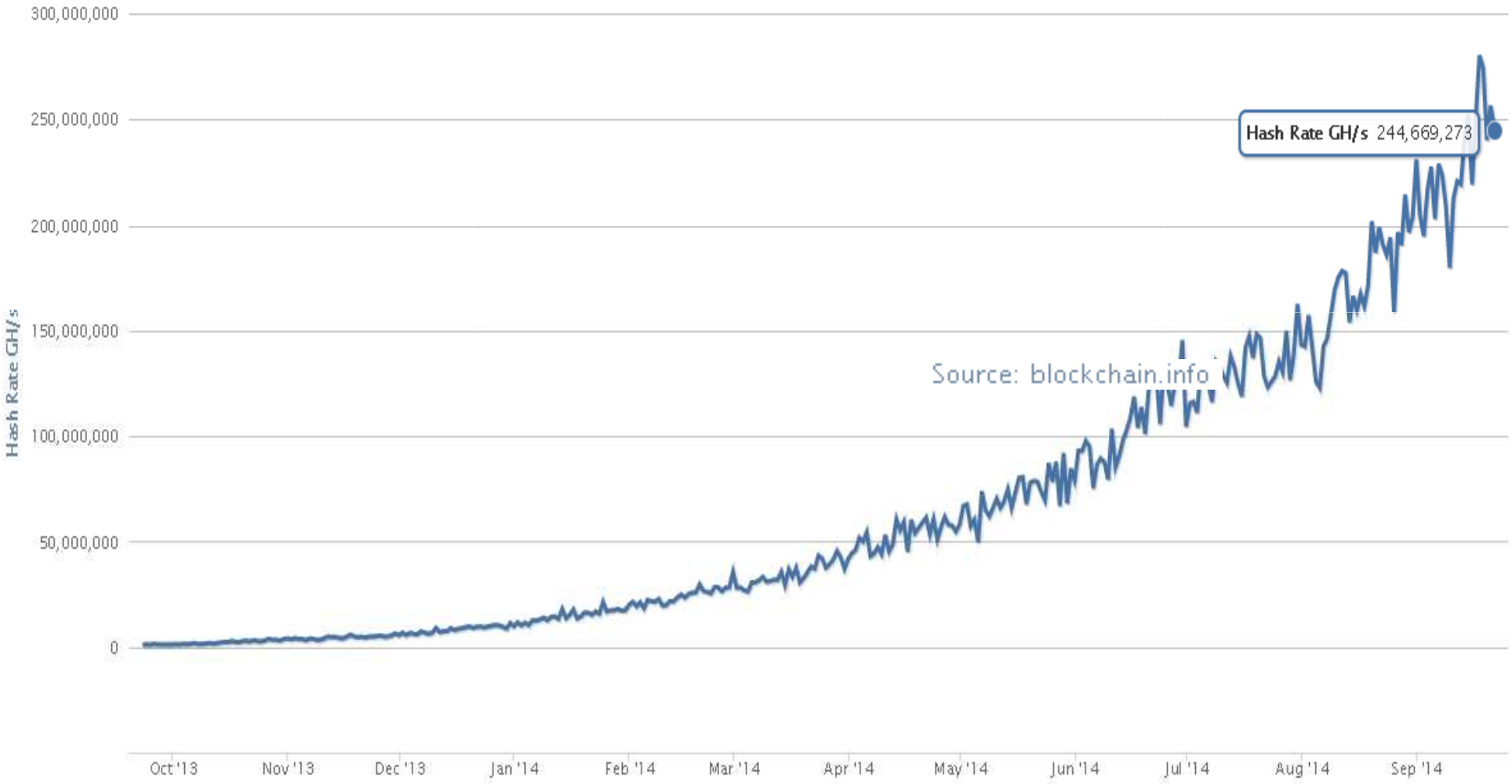
Like 1000% per year improvement.

Hash Rate - Doubled Nearly Every Month!

1000x in 1Y



Recently Still +60% Every Month



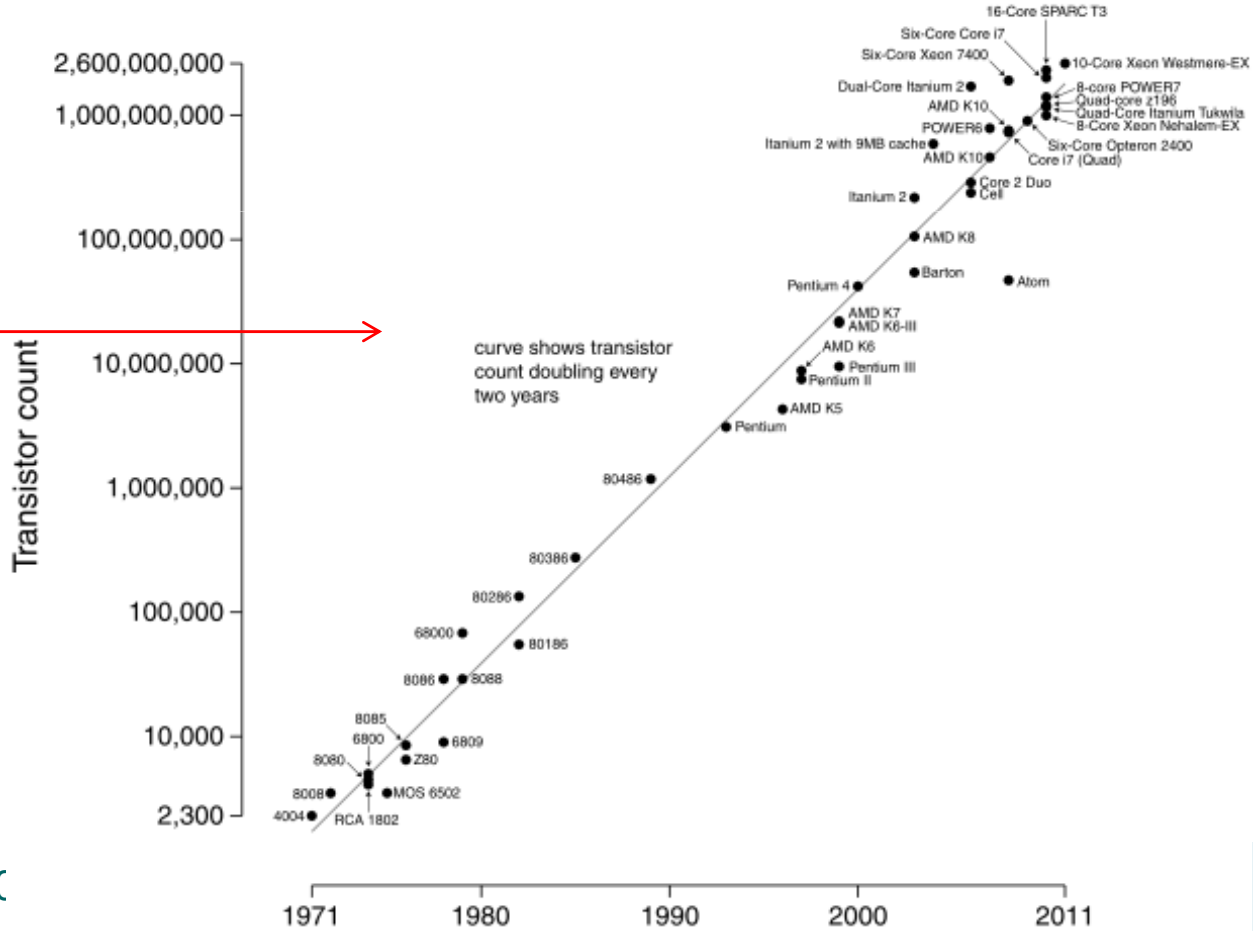
Five Generations of Miners!

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

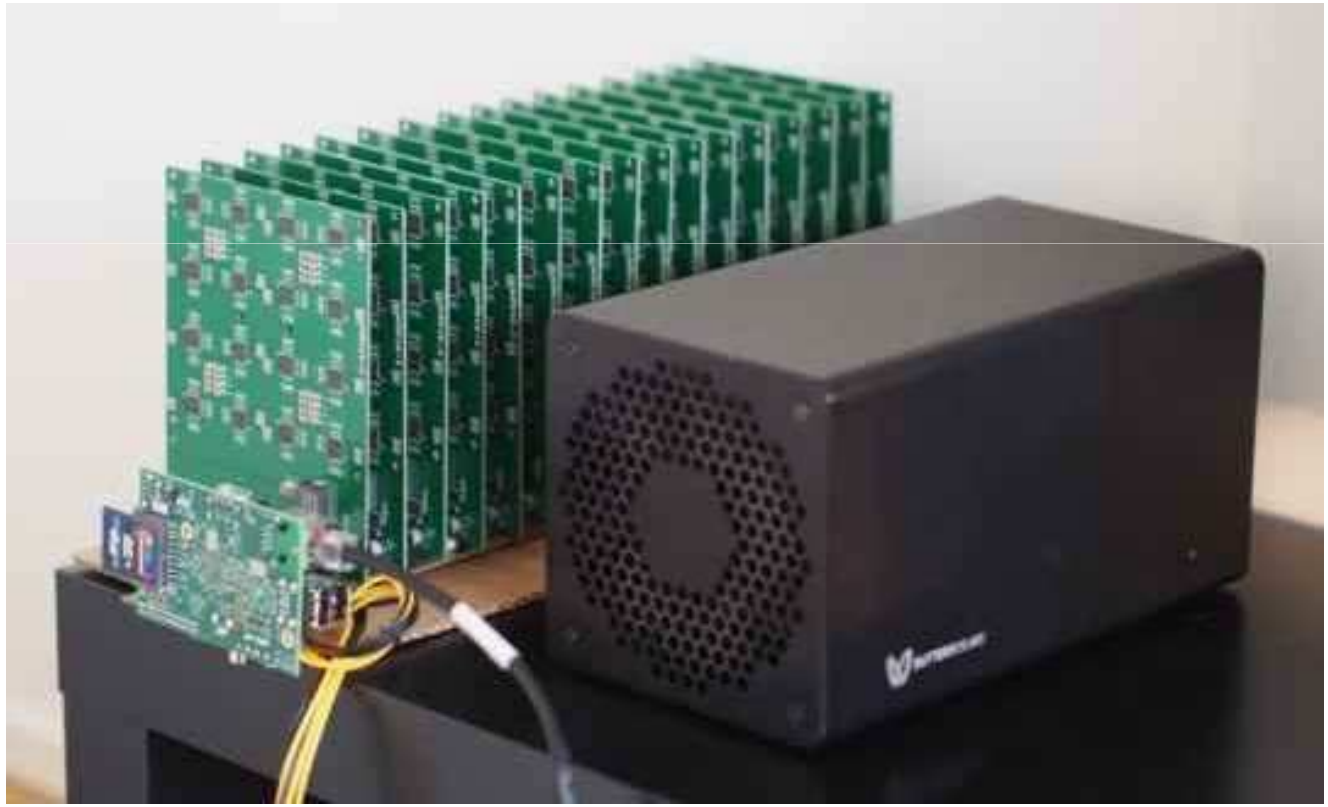
BUTTERFLYLABS

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



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

ASICs Comparison

By power / Gh/s

0.35 W low power mode

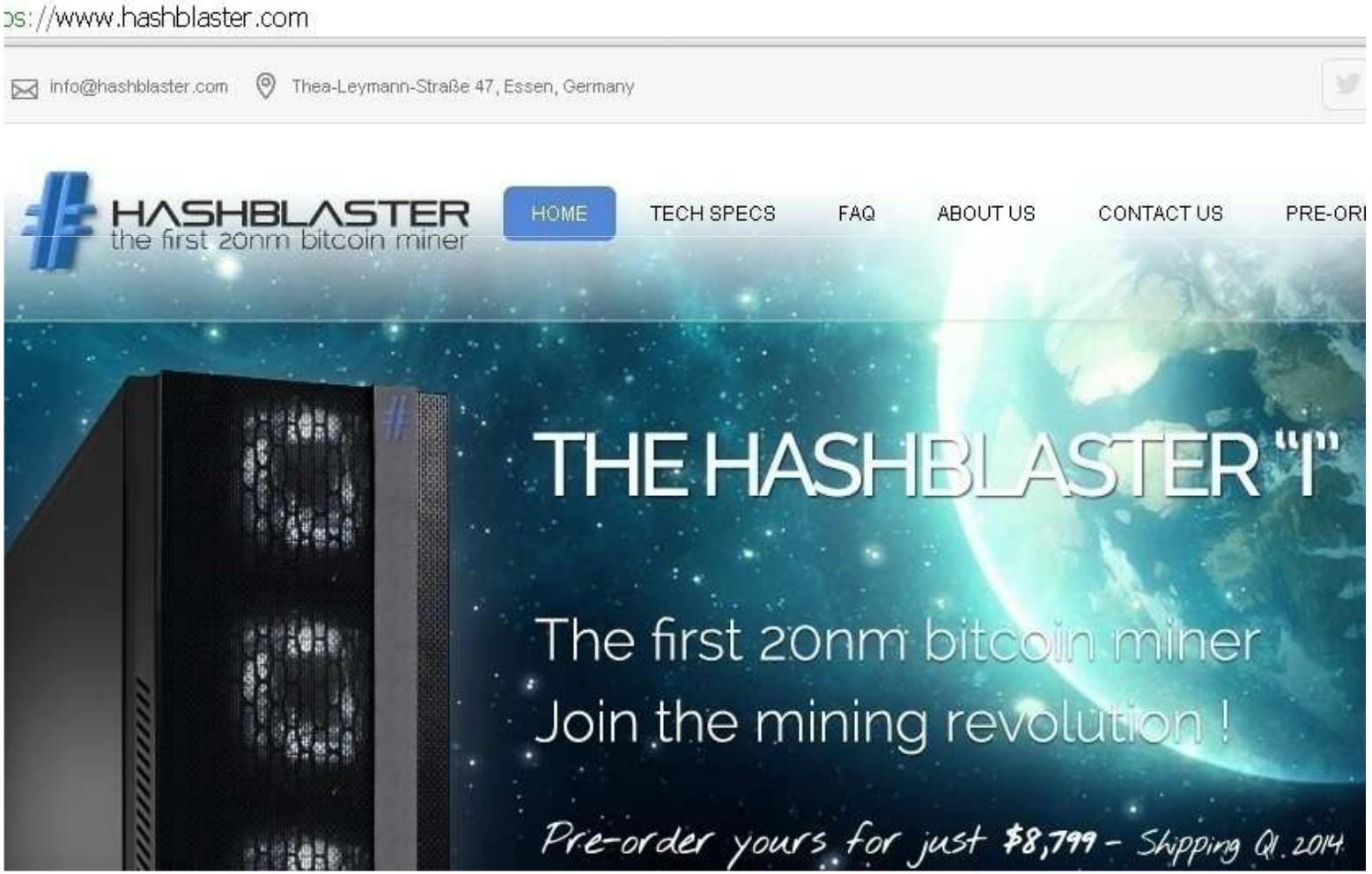
BITMINE.CH
For serious miners

1 W KnCMiner

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

Criminal Scams

See bitcoinscammers.com



Immoral Business Practice

I do not now 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…

Miners and Poland

Carlson/MegaBigPower.com
has a Polish investor:
a Poland-based scientific
research center BioInfoBank

MegaBigPower.com
also run a pool:
12 PH/s as of 9/2014,
100K$/day

THE MINE

megabigpower.com/themine

MegaBigPower's mining operation is divided between locations in Poland and the United States. In the USA, we have nearly two petahash of bitcoin mining set up in eastern Washington State. The location was

New Miners

Cointerra Q1 2015:

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

$\Rightarrow$ 0.29 W per Gh/s

Total Cost? About 1.0 Billion USD

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

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

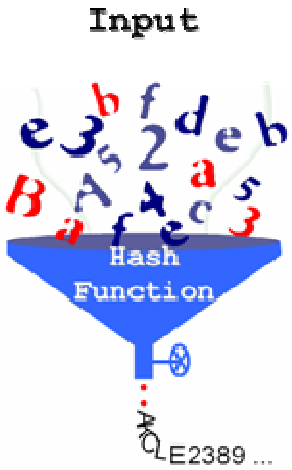
Assume most people use Neptune first generation which costed 3500 USD for 0.25 Th/s of hash power (better devices exist frankly just in pre-orders, well for a majority of people).

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

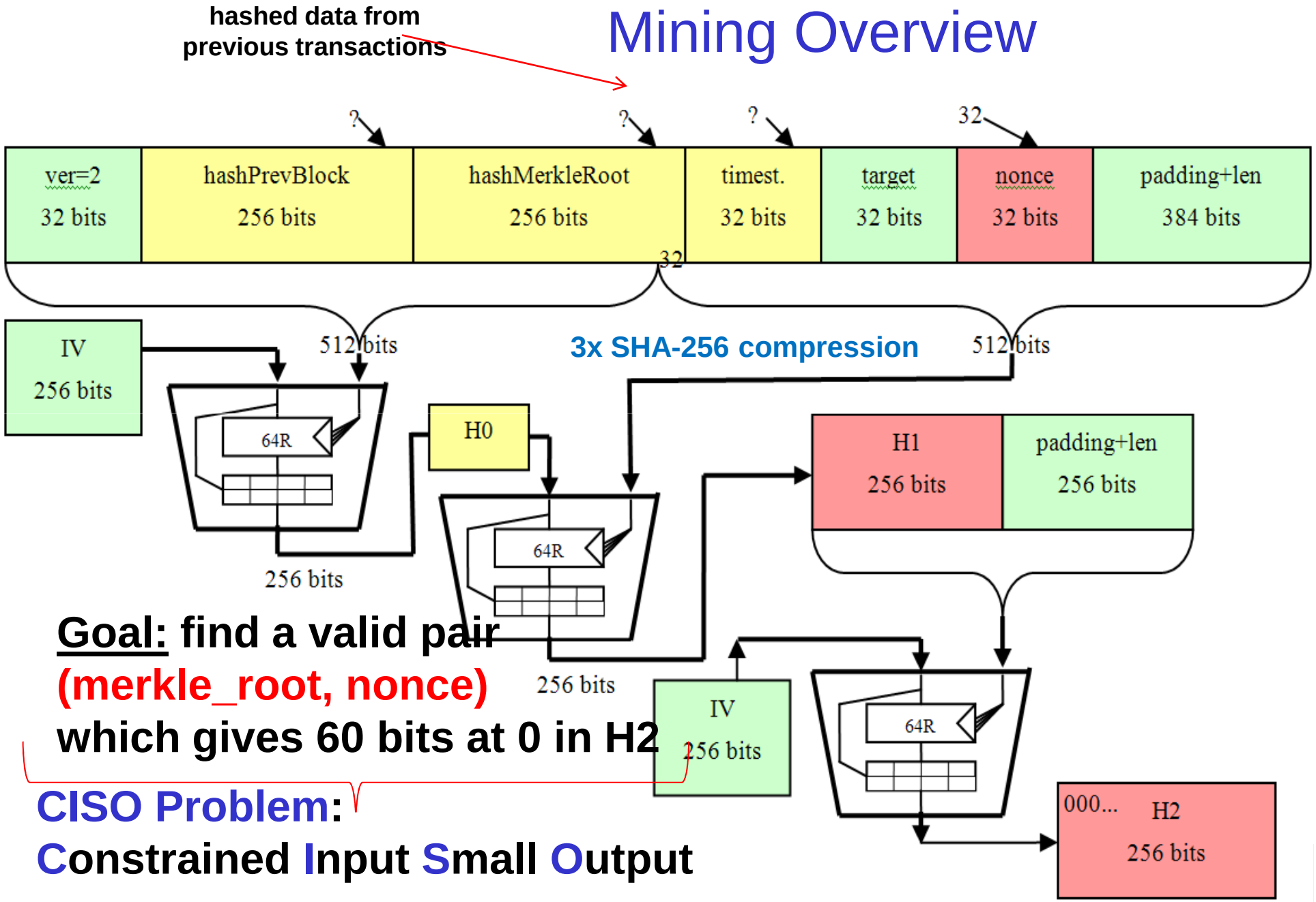
However probably most people still use miners NOT as good as Neptune, then probably this is 2 times more... So maybe it is already more than 1 billion today.

600 M / 100 K people = 6000 USD typical investment?

Bitcoin
And Hash Functions



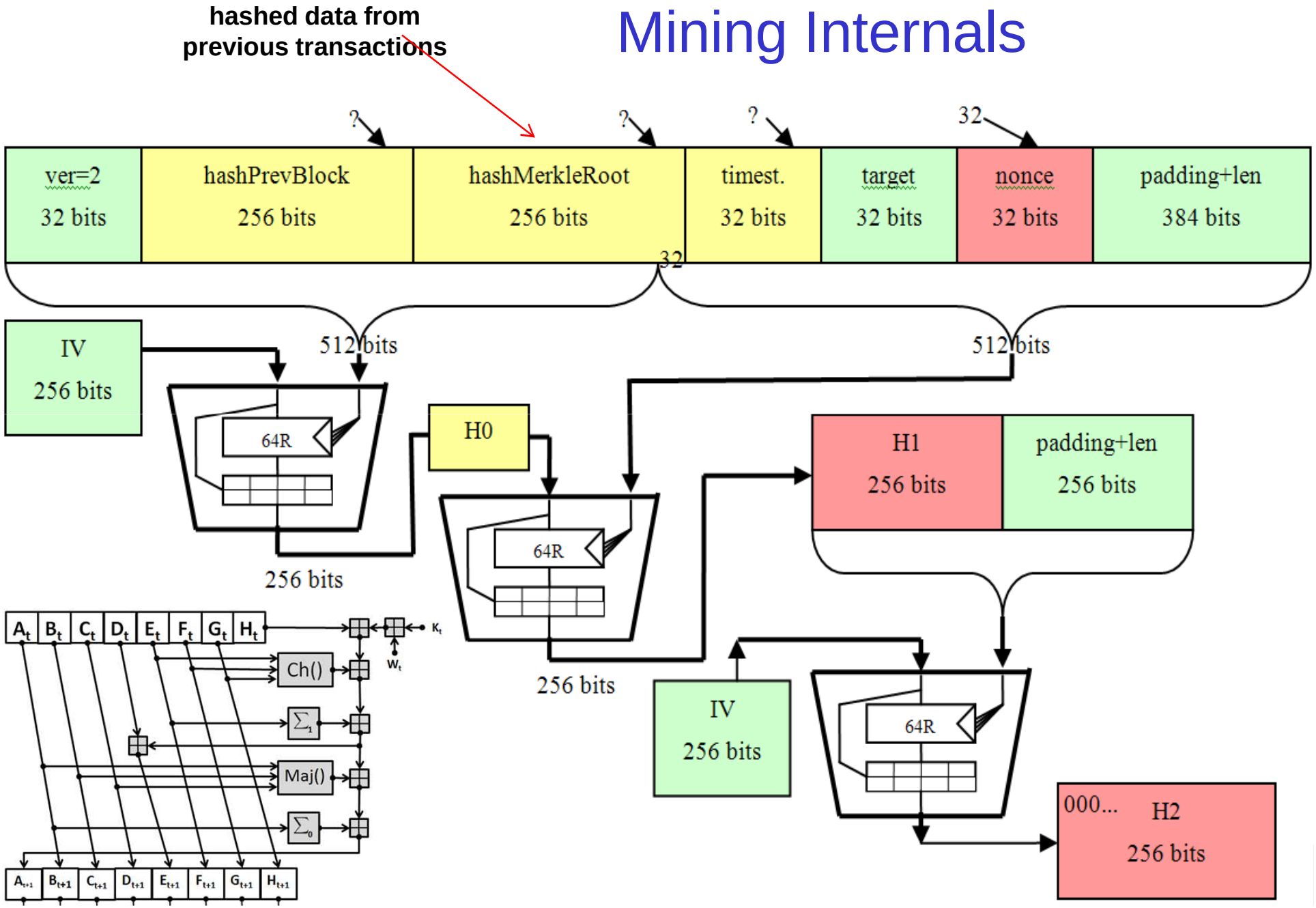
Mining Overview



Goal: find a valid pair
(merkle_root, nonce)
which gives 60 bits at 0 in H2

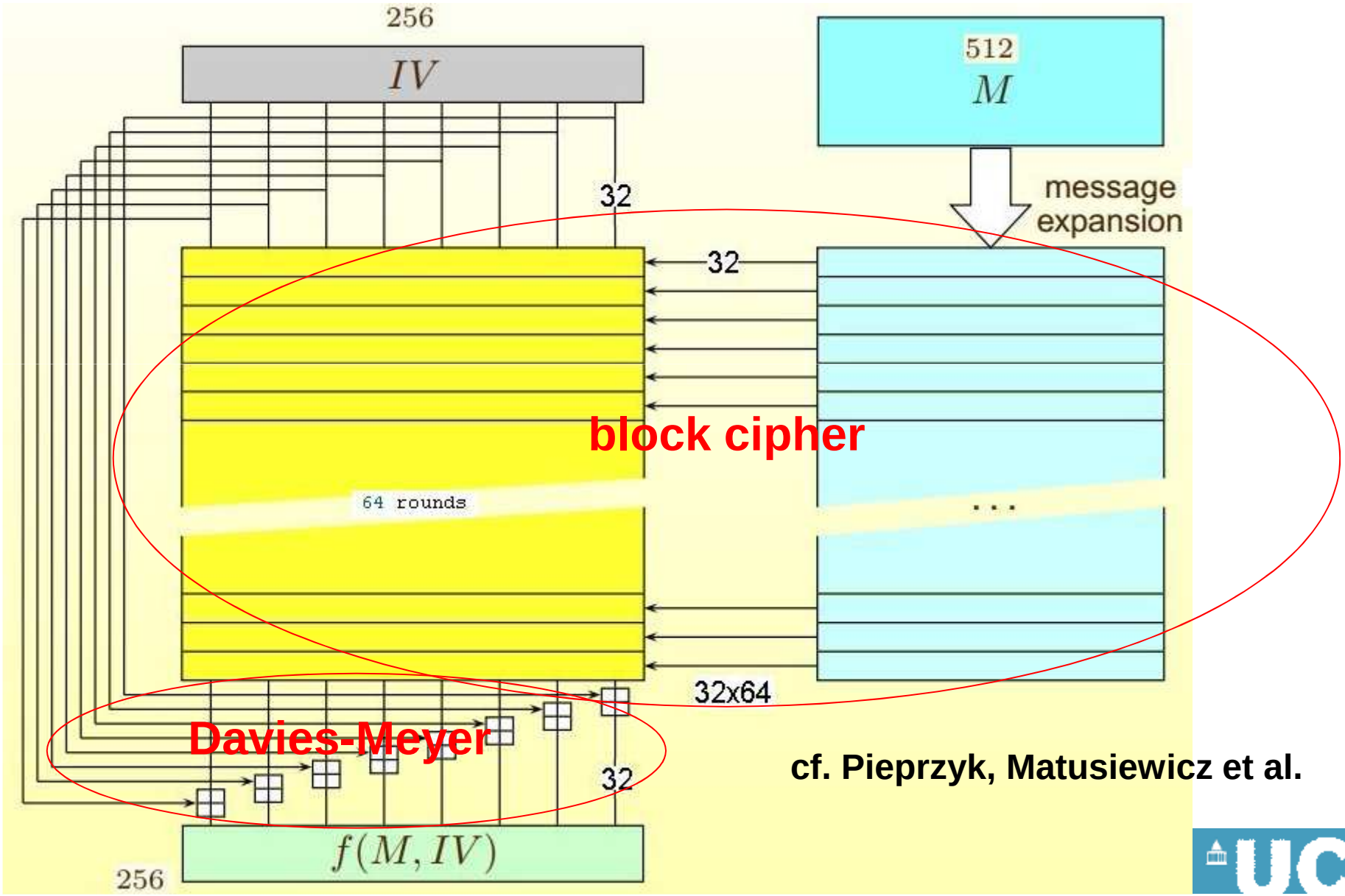
CISO Problem:
Constrained Input Small Output

Mining Internals



Bitcoin
Hash Functions
And Block Ciphers (!)

SHA-256 Compression Function

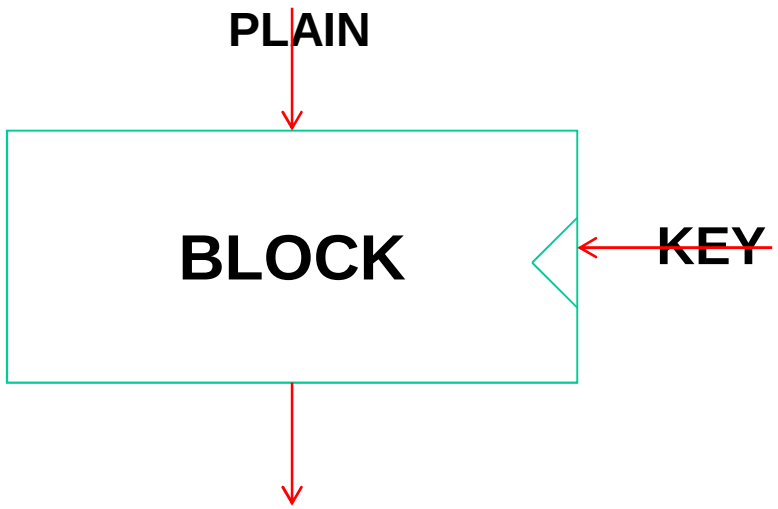


cf. Pieprzyk, Matusiewicz et al.

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.

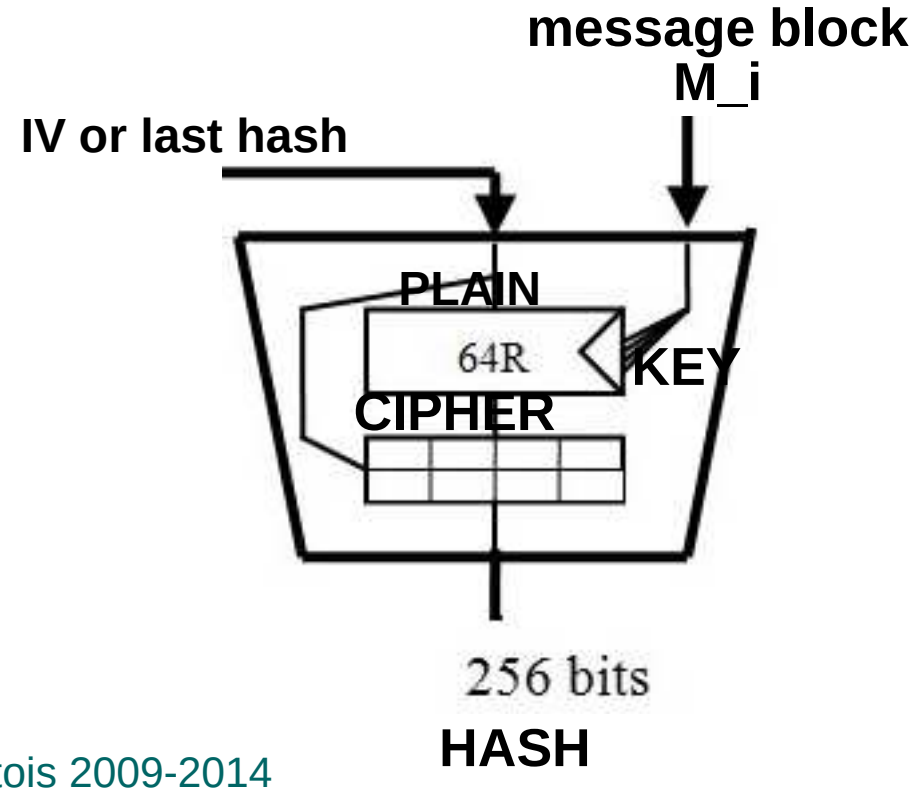


Davies-Meyer

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

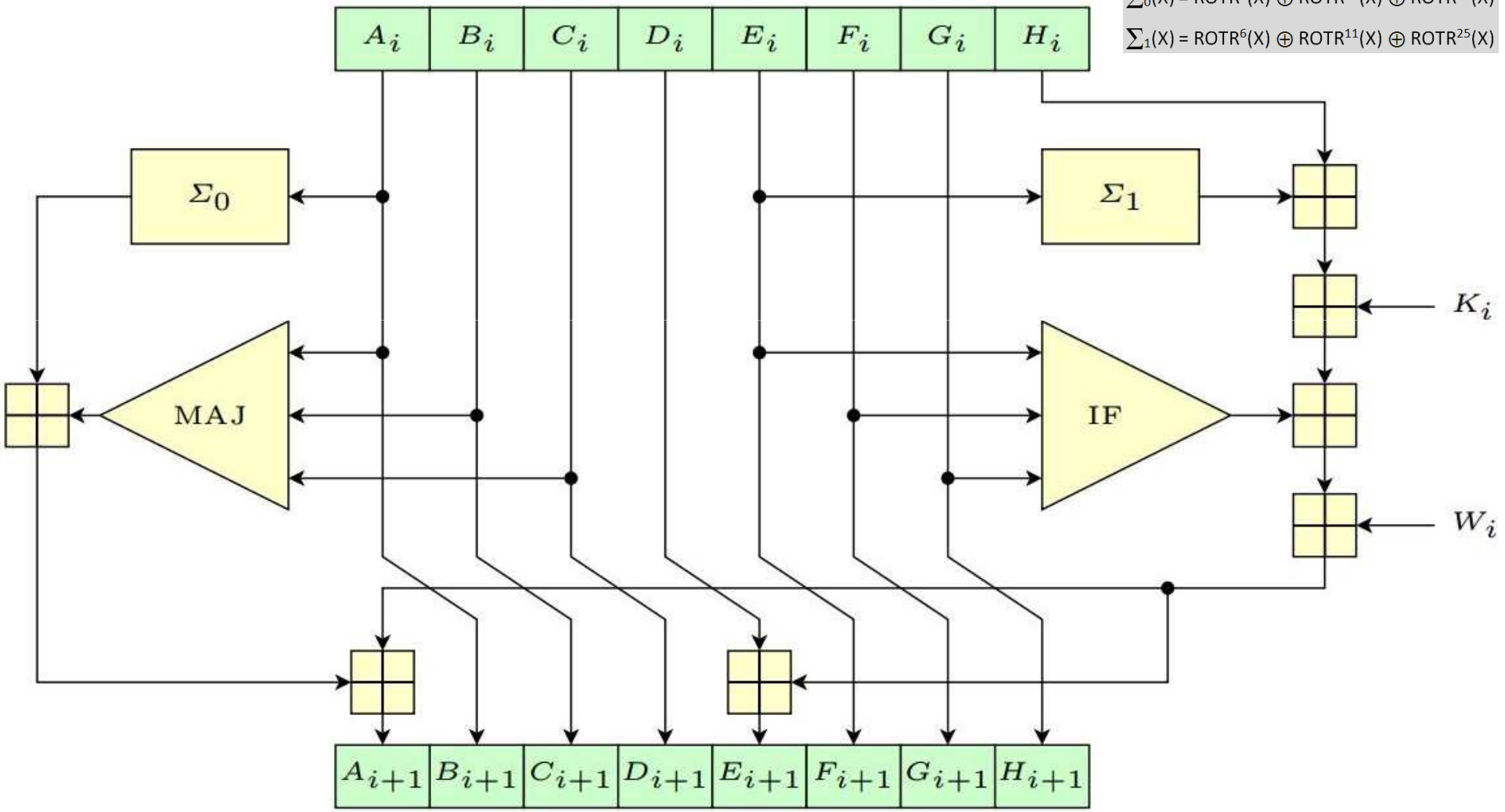
cf. Pieprzyk, Matusiewicz et al.

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

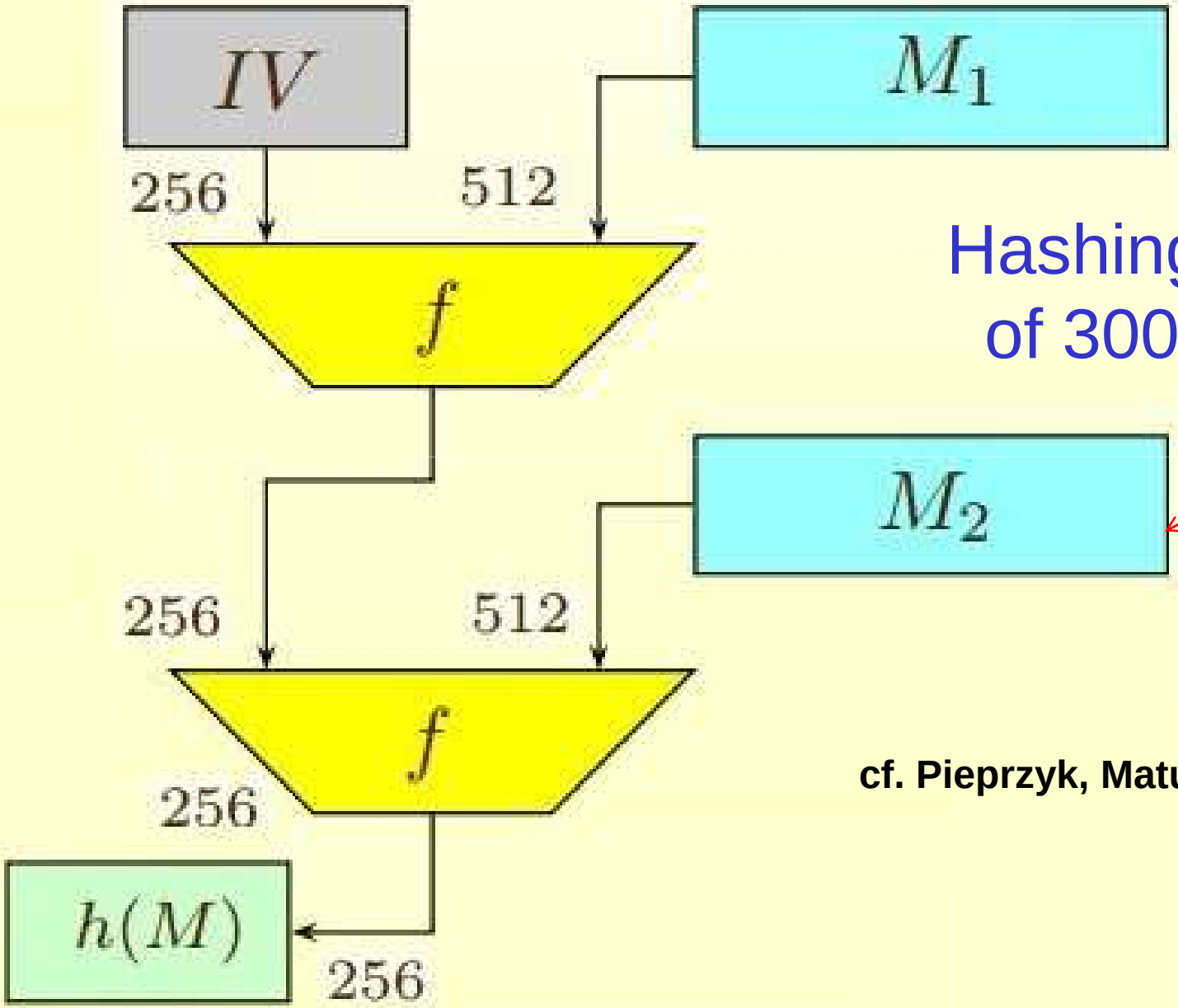
$Maj(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$

$\sum_0(X) = ROTR^2(X) \oplus ROTR^{13}(X) \oplus ROTR^{22}(X)$

$\sum_1(X) = ROTR^6(X) \oplus ROTR^{11}(X) \oplus ROTR^{25}(X)$



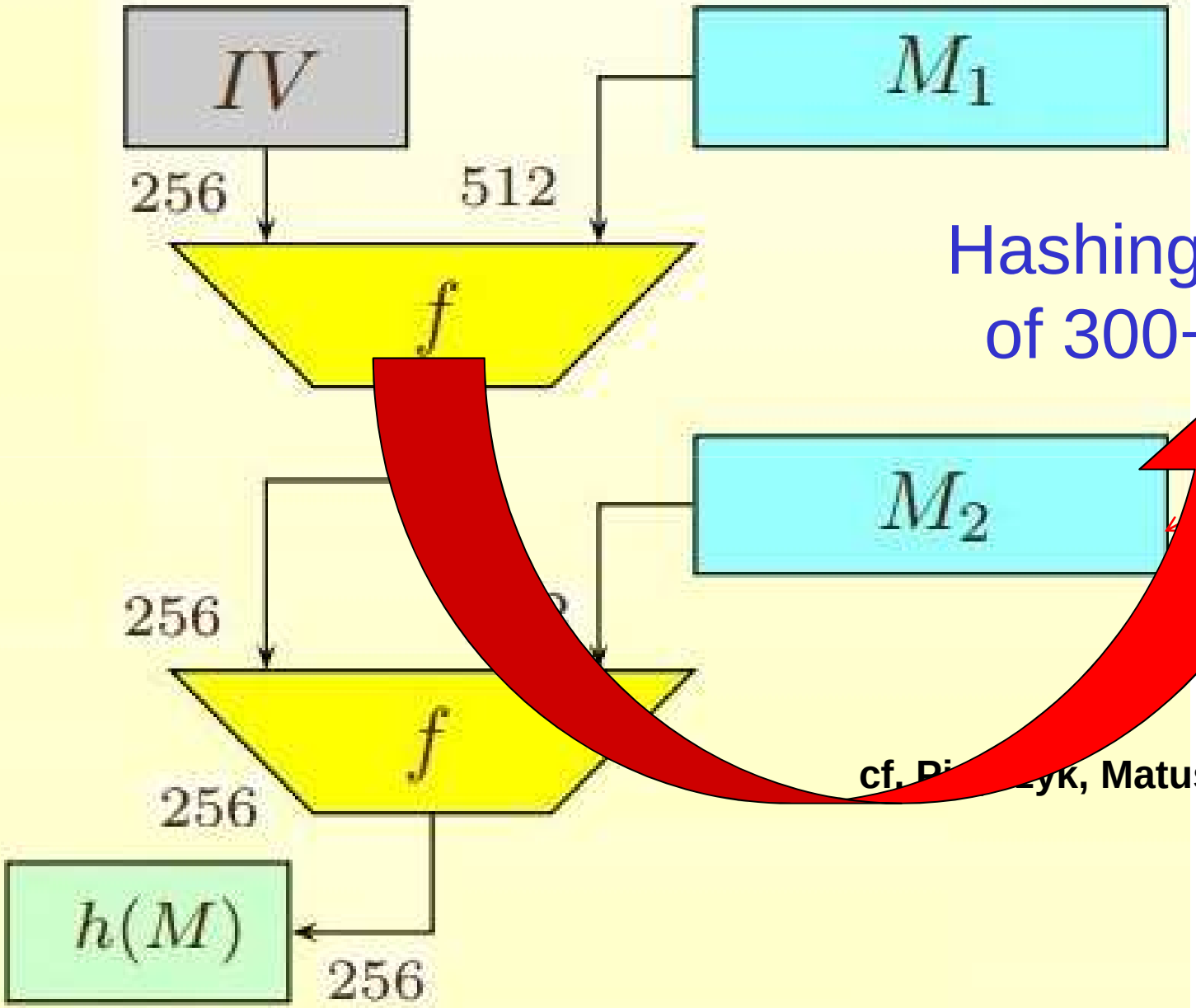
Optimising Mining
(39% gain w.r.t. best ASIC)
Like Generation 4.1.



Hashing Block of 300+ Bits

padding added

cf. Pieprzyk, Matusiewicz et al.

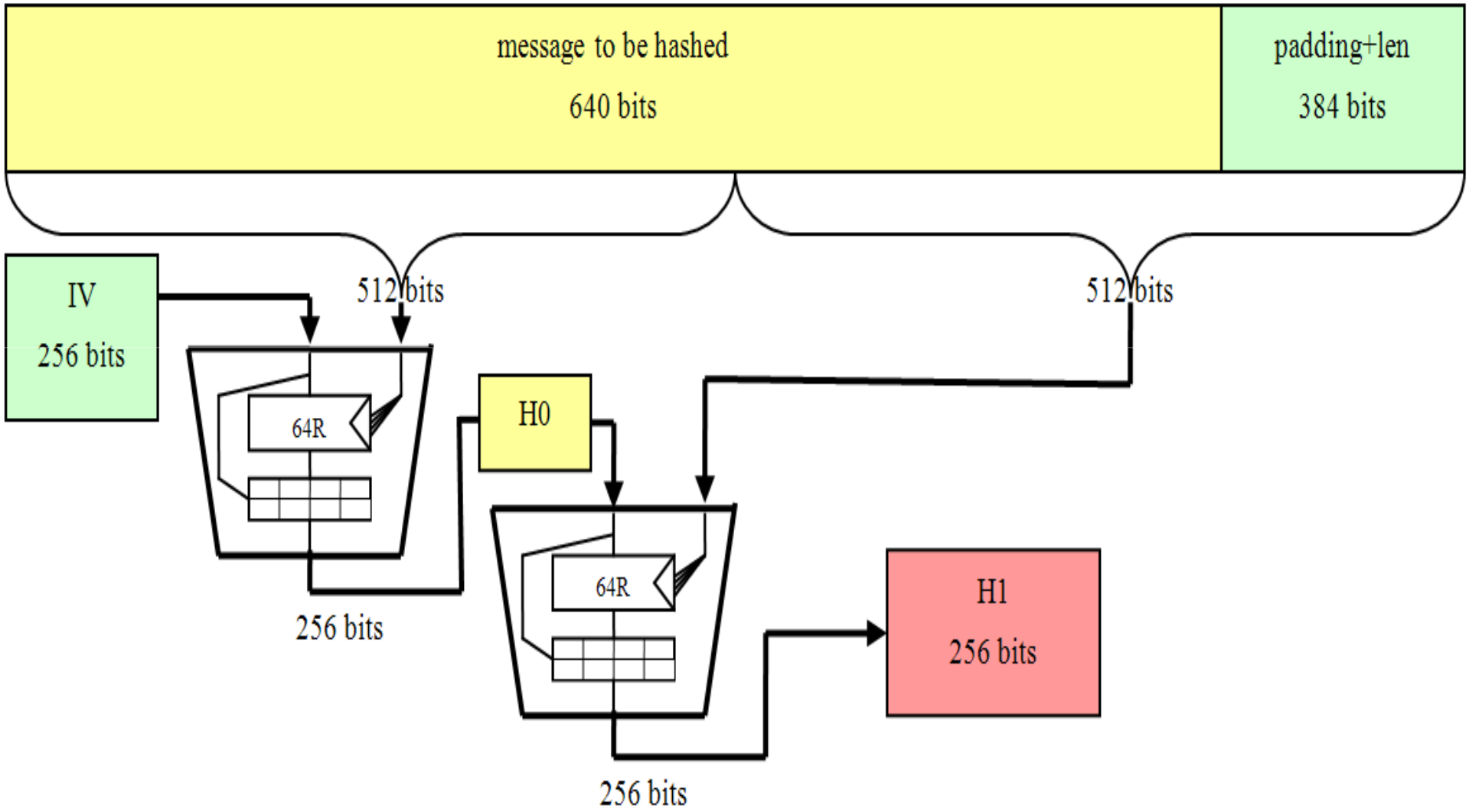


Hashing Block of 300+ Bits

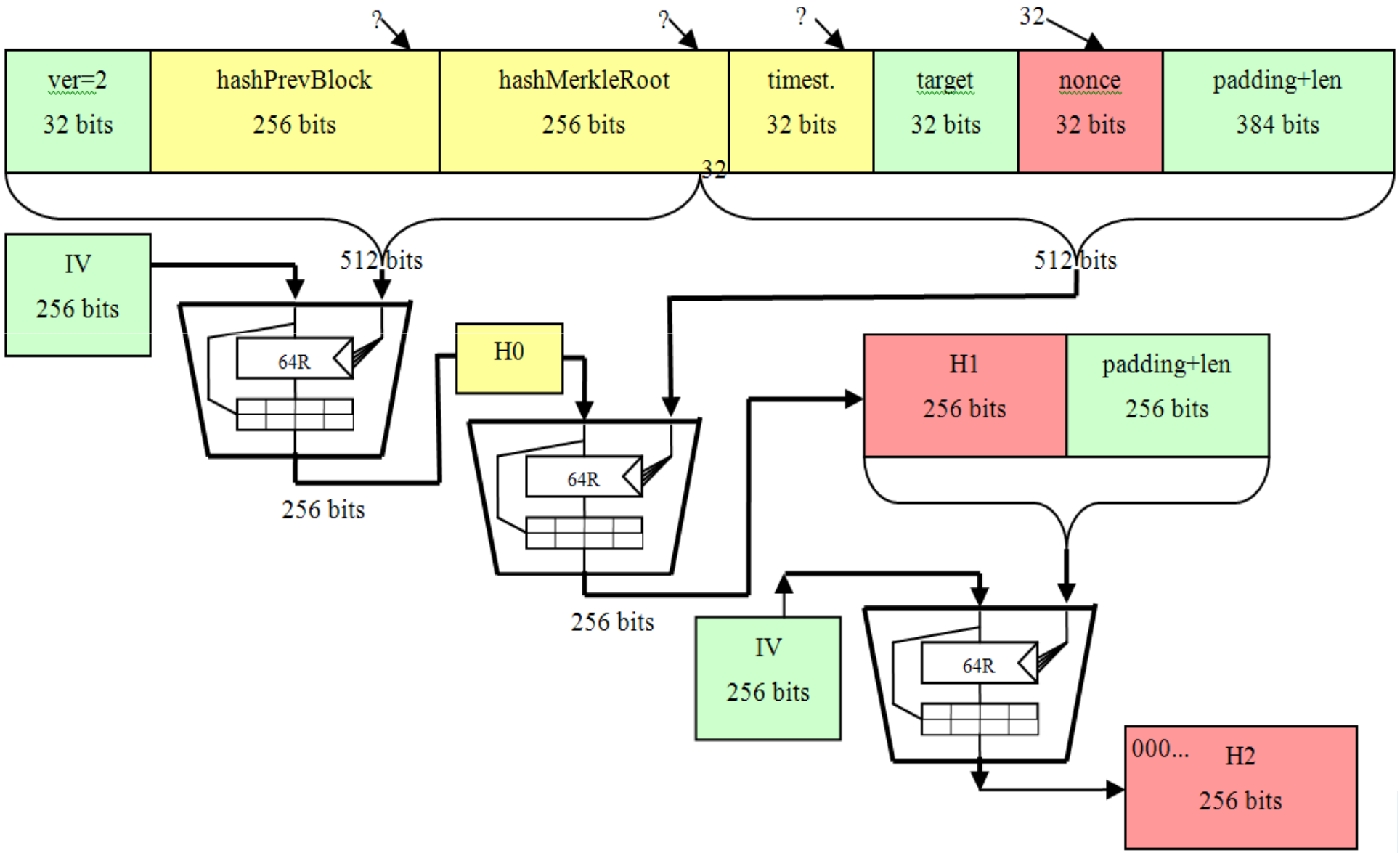
ng added

cf. Pi yk, Matusiewicz et al.

Padding


message to be hashed
640 bits
padding+len
384 bits
IV
256 bits
512 bits
512 bits
64R
H0
64R
H1
256 bits
256 bits
256 bits

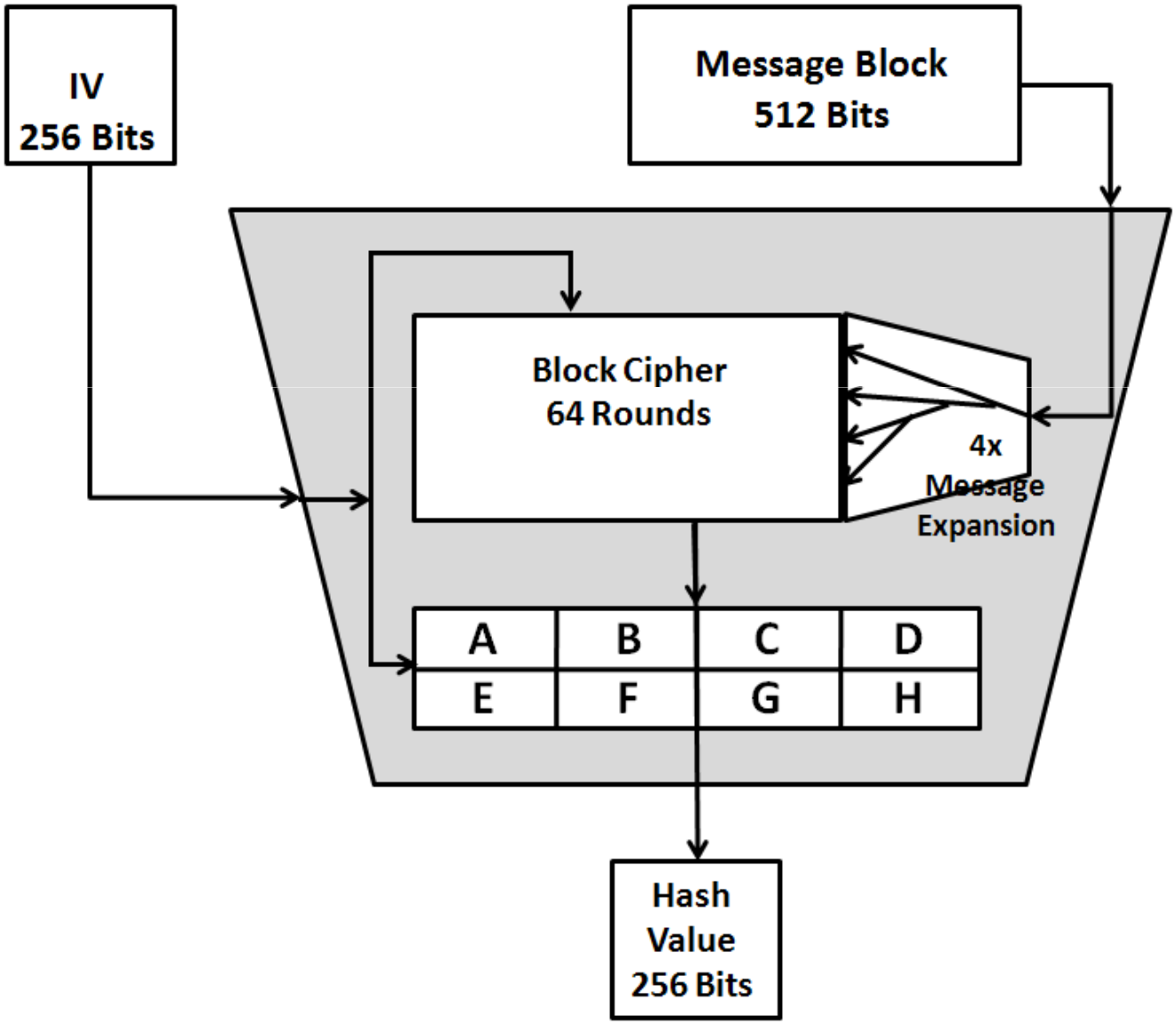
+ Second Hash


?
?
?
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
IV
256 bits
512 bits
512 bits
64R
H0
256 bits
64R
H1
256 bits
padding+len
256 bits
256 bits
IV
256 bits
64R
000...
H2
256 bits

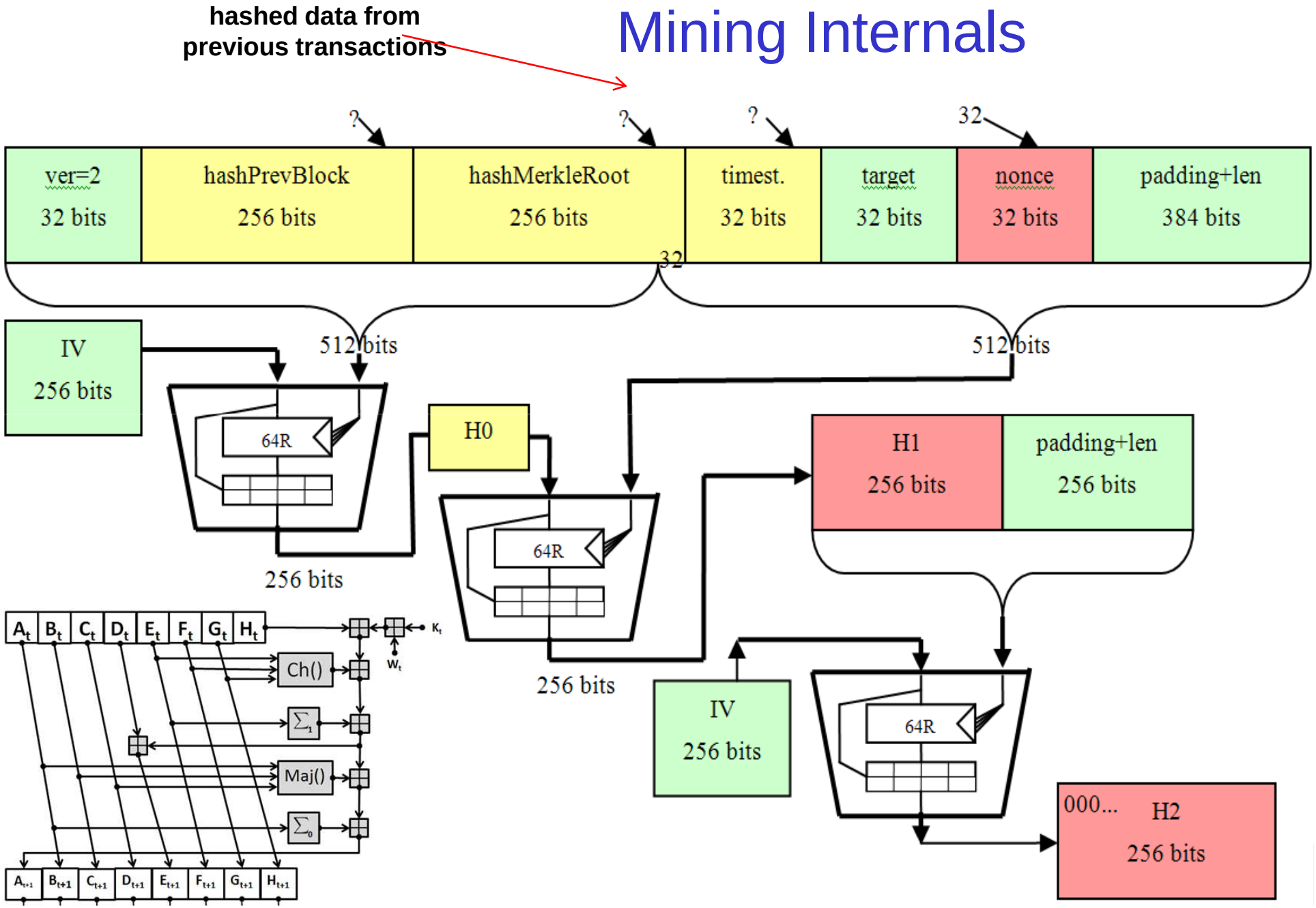
Inputs

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 + len	384 bits	standard fixed SHA256 padding on 384 bits for Len=640 bits

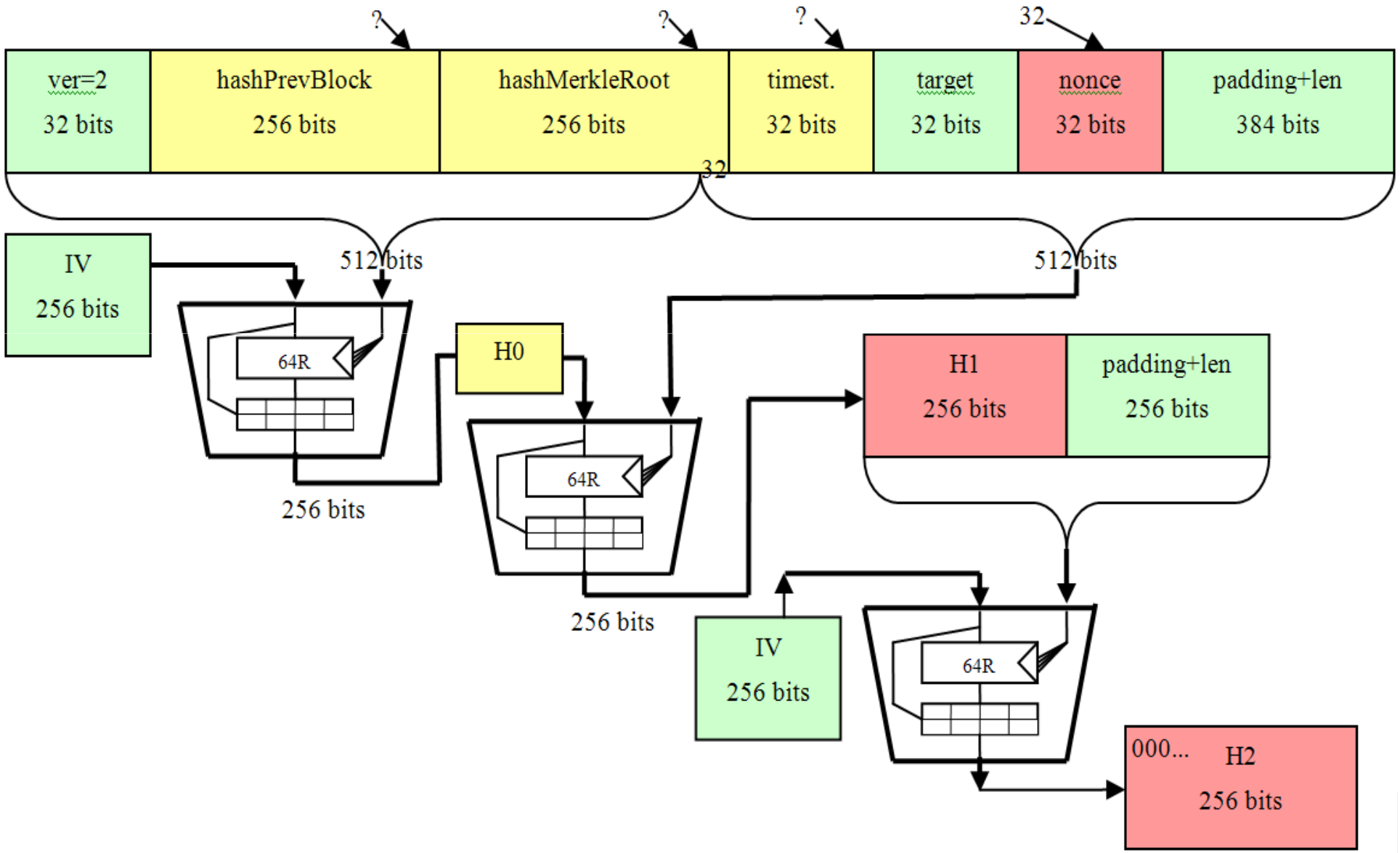
Davies-Meyer



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

UCL

Improvement 4 – Incremental Computation

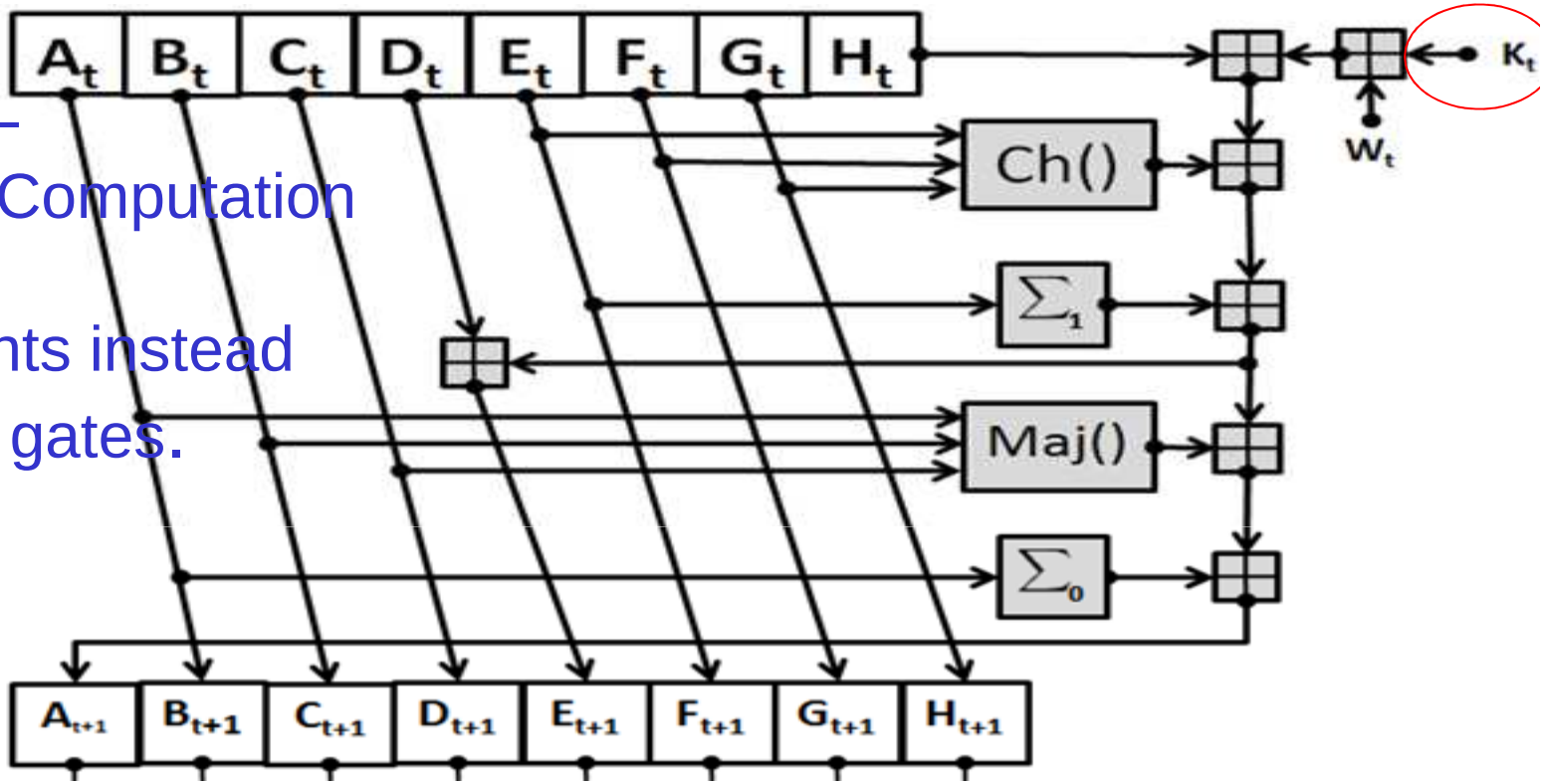
computation of H1		
Round t	32 bit W_t	Description
0	XXXXXXXX	last 32 Bits of hashMerkleRoot
1	XXXXXXXX	timestamp
2	XXXXXXXX	target
3	XXXXXXXX	nonce (00000000 to FFFFFFFF)
4	0x80000000	padding starts
5	0x00000000	|
6	0x00000000	|
7	0x00000000	|
8	0x00000000	|
9	0x00000000	|
10	0x00000000	|
11	0x00000000	|
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

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

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

$\sum_0(X) = ROTR^2(X) \oplus ROTR^{13}(X) \oplus ROTR^{22}(X)$

$\sum_1(X) = ROTR^6(X) \oplus ROTR^{11}(X) \oplus ROTR^{25}(X)$

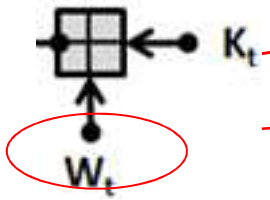
Improvement 5

–

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

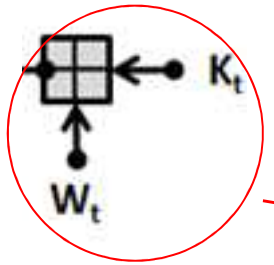
computation of H2		
Round t	32 bit W_t	Description
0	XXXXXXXX	$H1_0$
1	XXXXXXXX	$H1_1$
2	XXXXXXXX	$H1_2$
3	XXXXXXXX	$H1_3$
4	XXXXXXXX	$H1_4$
5	XXXXXXXX	$H1_5$
6	XXXXXXXX	$H1_6$
7	XXXXXXXX	$H1_7$
8	0x80000000	Padding Starts
9	0x00000000	|
10	0x00000000	|
11	0x00000000	|
12	0x00000000	|
13	0x00000000	Padding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

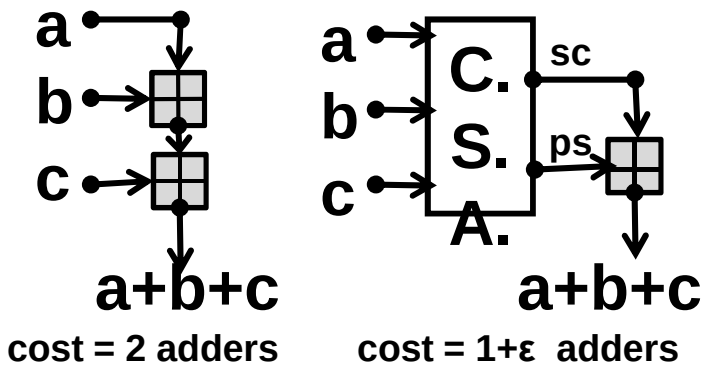


computation of H1		
Round t	32 bit W_t	Description
0	XXXXXXXX	last 32 Bits of hashMerkleRoot
1	XXXXXXXX	timestamp
2	XXXXXXXX	target
3	XXXXXXXX	nonce (00000000 to FFFFFFFF)
4	0x80000000	padding starts
5	0x00000000	|
6	0x00000000	|
7	0x00000000	|
8	0x00000000	|
9	0x00000000	|
10	0x00000000	|
11	0x00000000	|
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

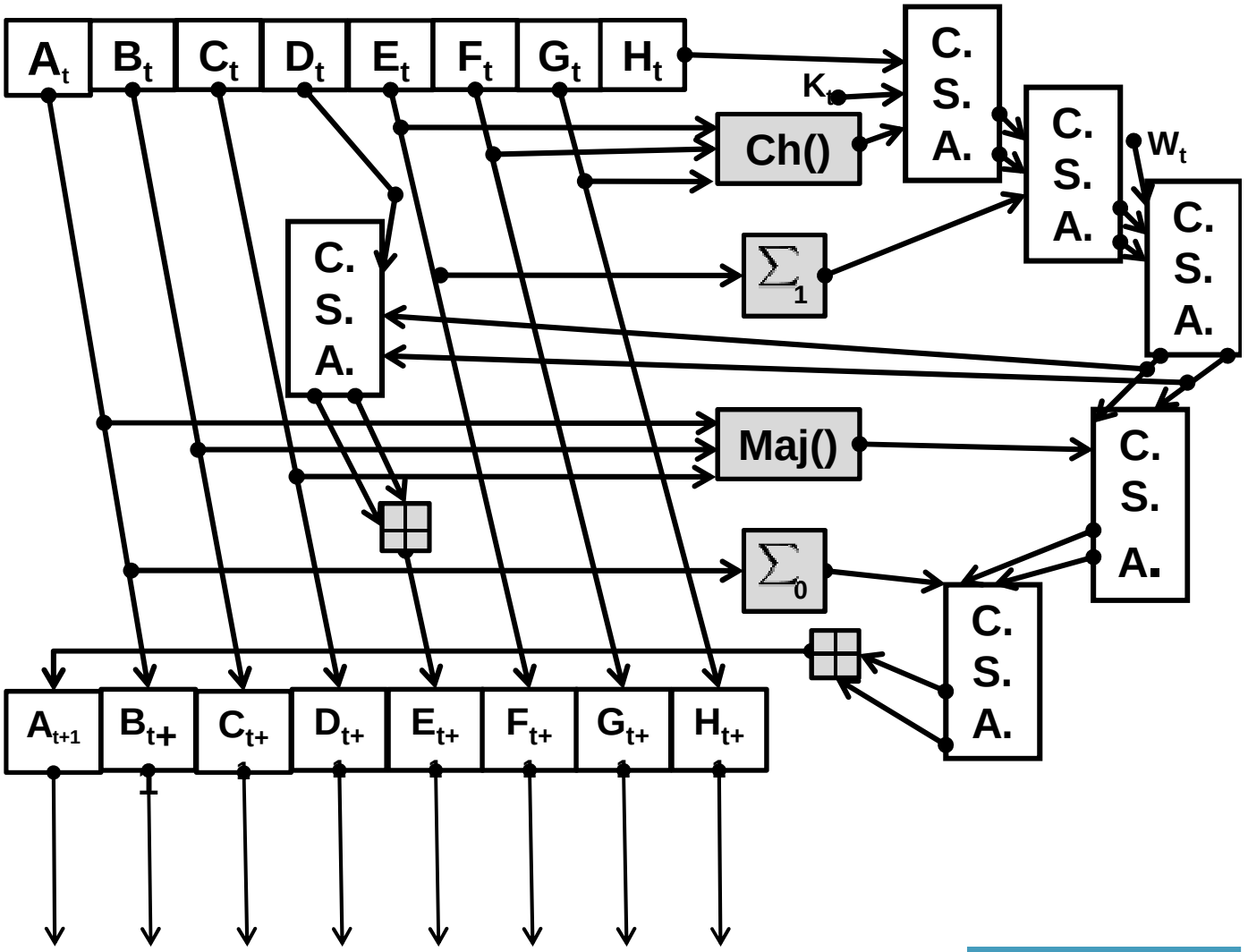
Improvement X

Classical trick: Carry Save Adders.



Whole Round

Only two full adders.



Message Schedule

For $0 \le t \le 15$,

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

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

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

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

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

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

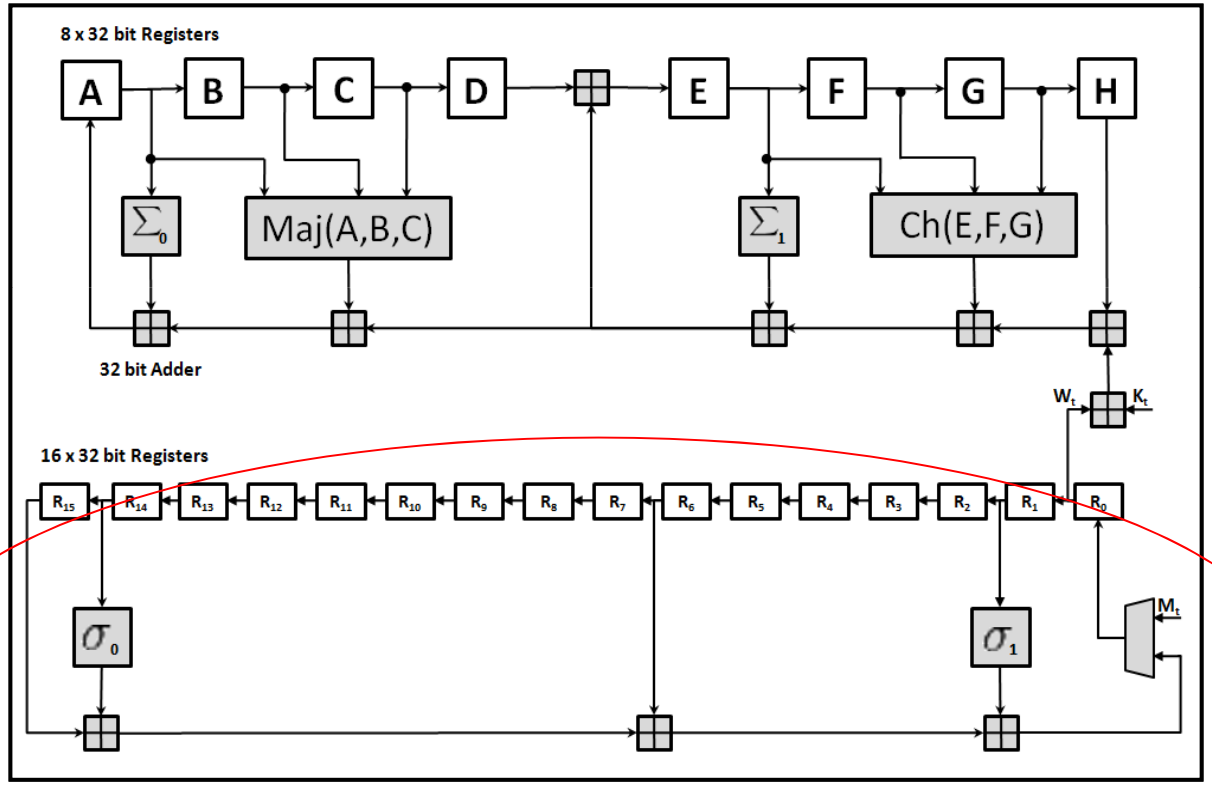
$\sigma_1(x) = ROTR^{17}(x) \oplus ROTR^{19}(x) \oplus SHR^{10}(x)$

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

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

$\sum_0(X) = ROTR^2(X) \oplus ROTR^{13}(X) \oplus ROTR^{22}(X)$

$\sum_1(X) = ROTR^6(X) \oplus ROTR^{11}(X) \oplus ROTR^{25}(X)$



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 H2 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

[claimed by Courtois just afterwards]:

NOBODY OWNS BITCOIN

We claim the contrary: any attempt to change the POW is close to impossible to enforce

I WAS RIGHT, it has NOT been changed.

Too much money at stake.