

Phase Transitions



Nicolas T. Courtois



- University College London, UK



Phase Transitions

Sudden rather than progressive. $50 \Rightarrow 51\%$



Phase Transitions?

Creation and Destruction!

Fast or slow...

Researcher: cryptocurrencies such as Bitcoin are
programmed to self destruct

Posted By: MrFusion [[Send E-Mail](#)]

Date: Saturday, 10-May-2014 23:05:41



*Politically Incorrect News
Stranger than Fiction
Usually True!*

UCL Bitcoin Seminar



a crypto currency **research** seminar

every **Thursday 17h00**, sometimes **16h00 or 18h00**
room and exact hour varies

public web page:

blog.bettercrypto.com / SEMINAR

or Google "UCL bitcoin seminar"

Dr. Nicolas T. Courtois

1. cryptologist and codebreaker



UNIVERSITY CIPHER CHAMPION

March 2013



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



Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

My Whole Life:

Tried to improve
the security baseline...

My Whole Life:

Tried to improve
the security baseline...

Crying Wolf!

51%, Elliptic Curve, OpenSSL...



It did NOT help,

The Wolf was allowed to operate



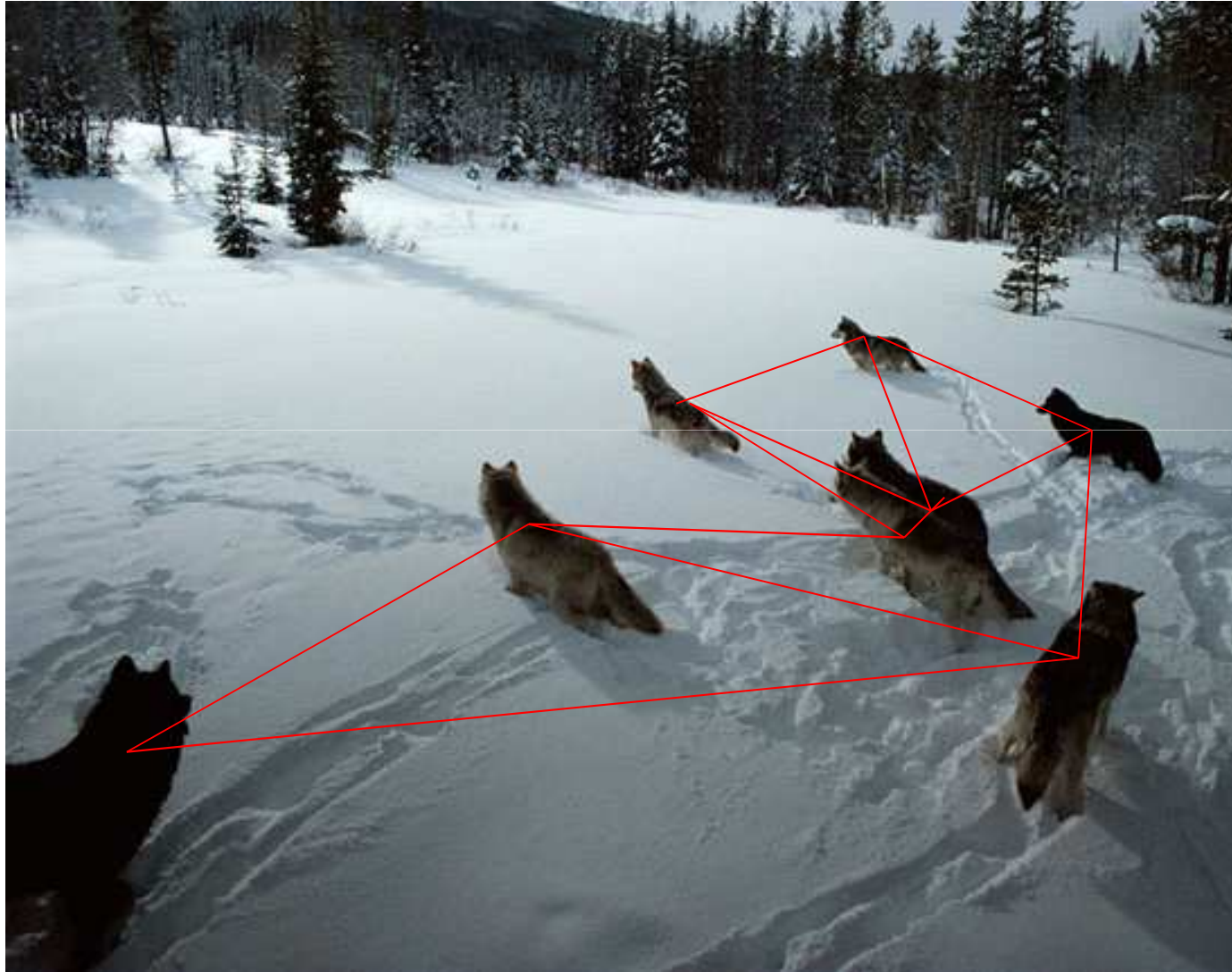
We failed to protect our DATA



We fail to protect our **MONEY**



Solution = Decentralized P2P



Solution = BlockChain



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

<http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html>

[11 June 2014]

The Telegraph

But Is Cryptography Incorruptible?

NSA 2013 Budget, excerpts:

[...] actively engages the US and foreign IT industries to **covertly influence** and/or overtly leverage their commercial products' designs.

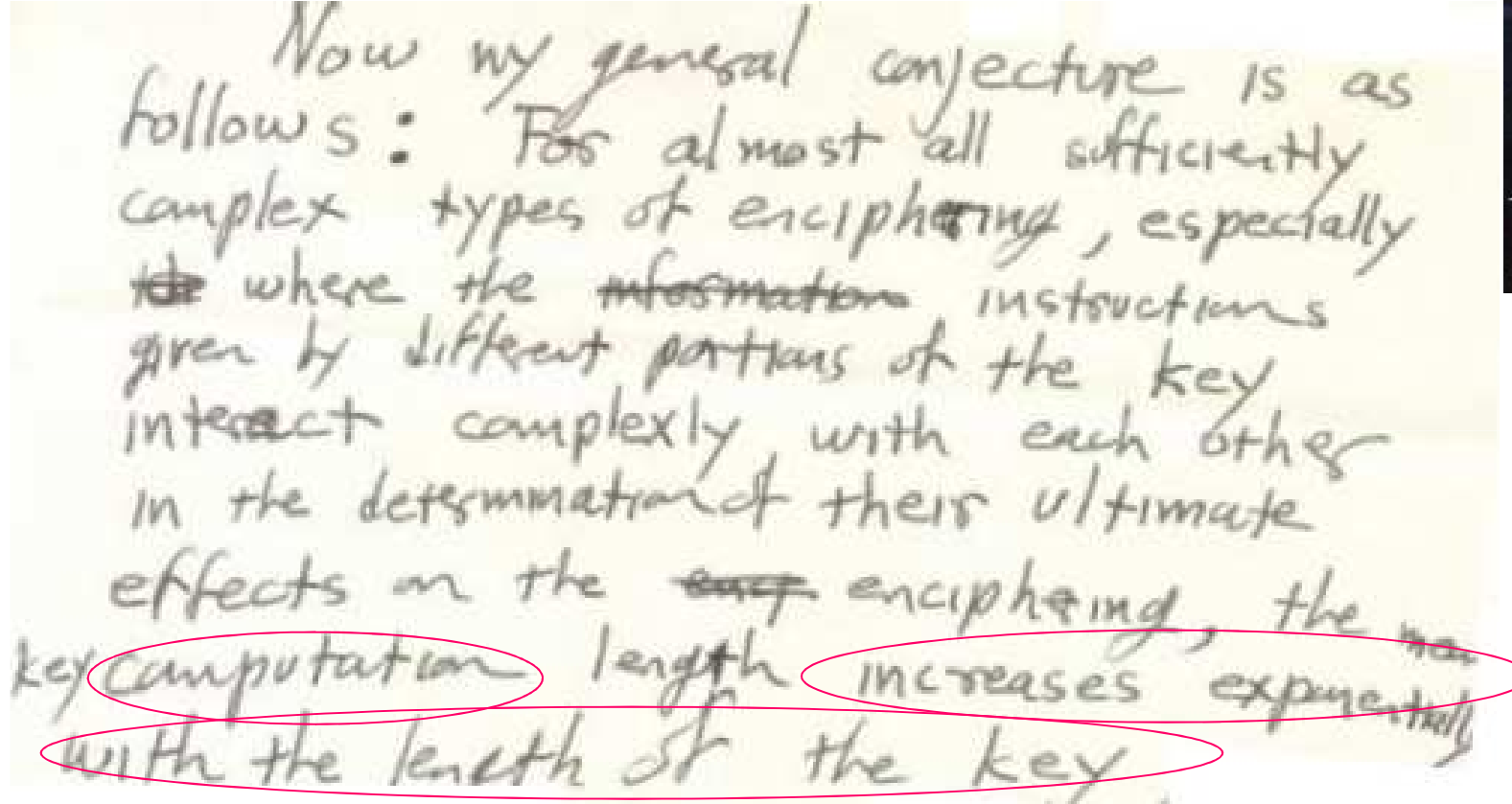


[...] **Insert vulnerabilities** into commercial encryption systems [...]

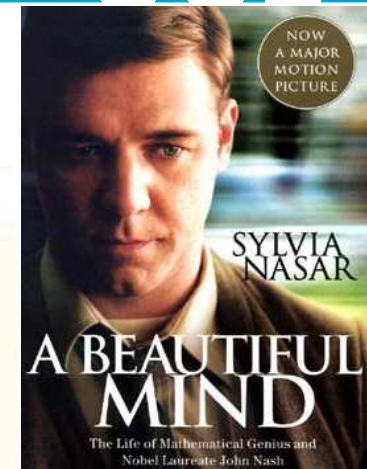
[...] Influence policies, standards and specification for commercial **public key technologies**. [...]

John Nash - 1955

In 2012 the NSA declassified his hand-written letter:



Now my general conjecture is as follows: For almost all sufficiently complex types of enciphering, especially ~~the~~ where the ~~information~~ instructions given by different portions of the key interact complexly with each other in the determination of their ultimate effects on the ~~enc~~ enciphering, the key computation length increases exponentially with the length of the key.

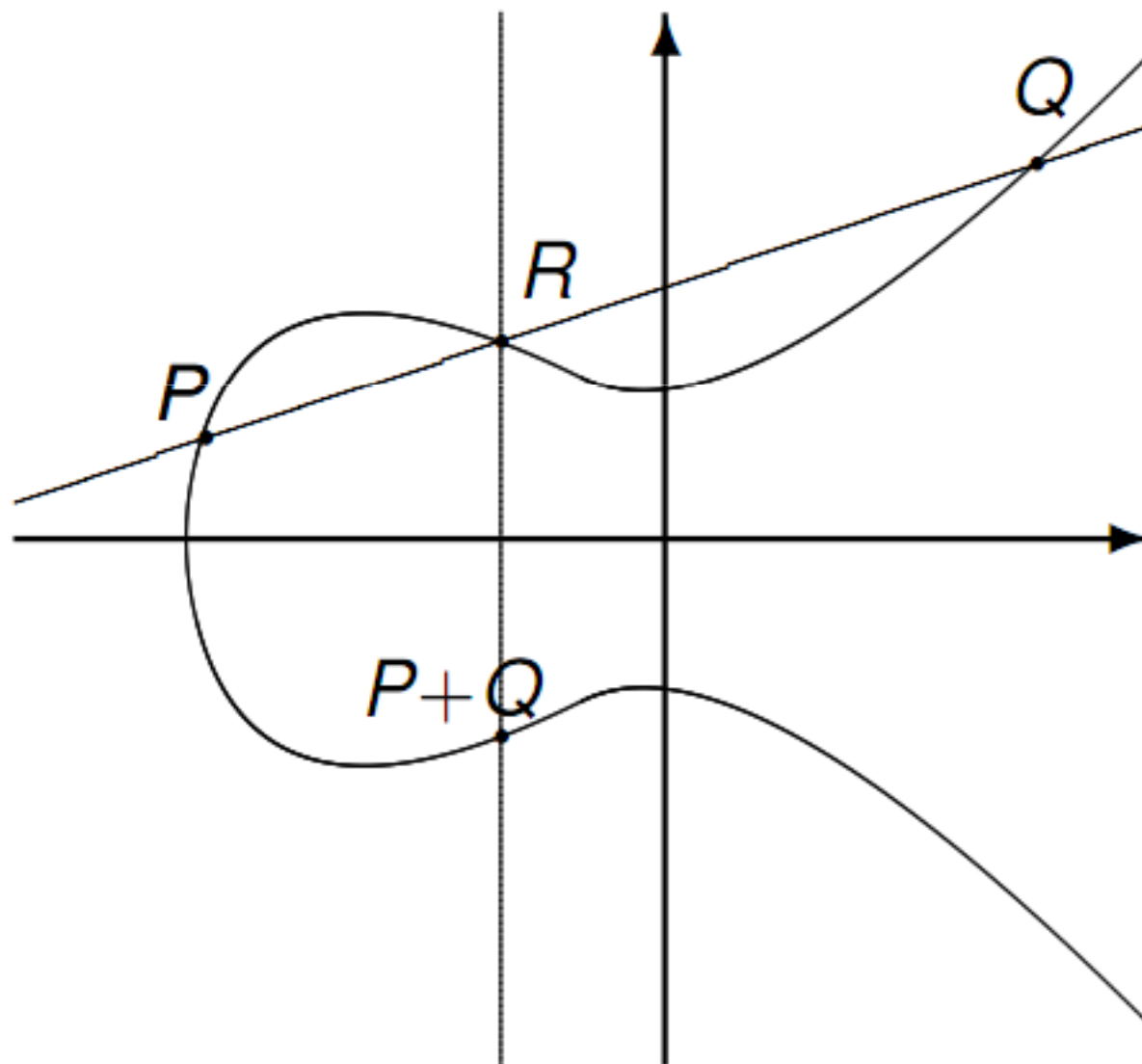


He also says that:

[...] the game of cipher breaking by skilled teams, etc., should become a thing of the past." [...]

Elliptic Curve Crypto

“exponential
security”



ECC - Certicom Challenges [1997, revised 2009]

ECC2K-95	97	18322	\$ 5,000
ECC2-97	97	180448	\$ 5,000

ECCp-97	97	71982	\$ 5,000
---------	----	-------	----------

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-108	109	1.3×10^6	\$10,000
ECC2-109	109	2.1×10^7	\$10,000
ECC2K-130	131	2.7×10^9	\$20,000
ECC2-131	131	6.6×10^{10}	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-109	109	9.0×10^6	\$10,000
ECCp-131	131	2.3×10^{10}	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-163	163	2.48×10^{15}	\$30,000
ECC2-163	163	2.48×10^{15}	\$30,000
ECC2-191	191	4.07×10^{19}	\$40,000
ECC2K-238	239	6.83×10^{26}	\$50,000
ECC2-238	239	6.83×10^{26}	\$50,000
ECC2K-358	359	7.88×10^{44}	\$100,000
ECC2-353	359	7.88×10^{44}	\$100,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-163	163	2.3×10^{15}	\$30,000
ECCp-191	192	4.8×10^{19}	\$40,000
ECCp-239	239	1.4×10^{27}	\$50,000
ECCp-359	359	3.7×10^{45}	\$100,000

TOTAL = 725,000 USD

Crypto Challenges:

I always liked this idea.

Claiming (very naive) that this would:

“punish those who
by their ignorance, incompetence
or because of a hidden agenda,
put everybody's security at a great risk.”

[Courtois, May 2006, Quo Vadis Cryptology 4 conference]

ECC - Certicom Challenges [1997, revised 2009]

ECC2K-95	97	18322	\$ 5,000
ECC2-97	97	180448	\$ 5,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-108	109	1.3×10^6	\$10,000
ECC2-109	109	2.1×10^7	\$10,000
ECC2K-130	131	2.7×10^9	\$20,000
ECC2-131	131	6.6×10^{10}	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECC2K-163	163	2.48×10^{15}	\$30,000
ECC2-163	163	2.48×10^{15}	\$30,000
ECC2-191	191	4.07×10^{19}	\$40,000
ECC2K-238	239	6.83×10^{26}	\$50,000
ECC2-238	239	6.83×10^{26}	\$50,000
ECC2K-358	359	7.88×10^{44}	\$100,000
ECC2-353	359	7.88×10^{44}	\$100,000

ECCp-97	97	71982	\$ 5,000
---------	----	-------	----------

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-109	109	9.0×10^6	\$10,000
ECCp-131	131	2.3×10^{10}	\$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US\$)
ECCp-163	163	2.3×10^{15}	\$30,000
ECCp-191	192	4.8×10^{19}	\$40,000
ECCp-239	239	1.4×10^{27}	\$50,000
ECCp-359	359	3.7×10^{45}	\$100,000

secp256k1
NOT INCLUDED
 no price if you
 break it ☹



Timely Denial

Dan Brown, chair of SEC [Certicom, Entrust, Fujitsu, Visa International...]

**“I did not know that BitCoin is using secp256k1.
I am surprised to see anybody use secp256k1 instead of secp256r1”,**

September 2013,

<https://bitcointalk.org/index.php?topic=289795.80>

Comparison:

Used/recommended by:	secp256k1	secp256r1
Bitcoin, anonymous founder, no one to blame...	Y	
SEC Certicom Research	surprised!	Y
TLS, OpenSSL	ever used???	Y 98.3% of EC
U.S. ANSI X9.63 for Financial Services	Y	Y
NSA suite B, NATO military crypto		Y
U.S. NIST		Y
IPSec		Y
OpenPGP		Y
Kerberos extension		Y
Microsoft implemented it in Vista and Longhorn		Y
EMV bank cards XDA [2013]		Y
German BSI federal gov. infosec agency, y=2015		Y
French national ANSSI agency beyond 2020		Y



Wanna Bet?

Bitcoin Cryptography Broken in 2015

Category: Bitcoin

By NCourtois ★★★★★

① Description

The digital signature scheme of bitcoin with SHA256+secp256k1 ECDSA will be broken before 1 September 2015 by cryptography researchers. The attack should allow to forge digital signatures for at least a proportion of 1/1 million bitcoin users and steal money from them. It should be done faster than 2^{100} point additions total including the time to examine the data.



⌚ Decision Logic



bitcoin, cryptography, SHA256, ECDSA, ECDL, secp256k1

<https://www.betmoose.com/bet/bitcoin-cryptography-broken-in-2015-791>

betmoose.com

Bitcoin Cryptography Broken in 2015

By NCourtois ★★★★★

The digital signature scheme of bitcoin with SHA256+secp256k1 ECDSA will be broken before 1 September 2015 by cryptography researchers.

The attack should allow to forge digital signatures for at least a proportion of 1/1 million bitcoin users and steal money from them.

It should be done faster than 2^{100} point additions total including the time to examine the data.

NO

Volume:	₿ 0.189
# of Bets:	6

₿ 0.1

PAYOUT	ROI
₿0.14327	43.27%

* assumes current weight and volumes

Place Anonymously



SHA256, ECDSA, ECDL, secp256k1

Amount?

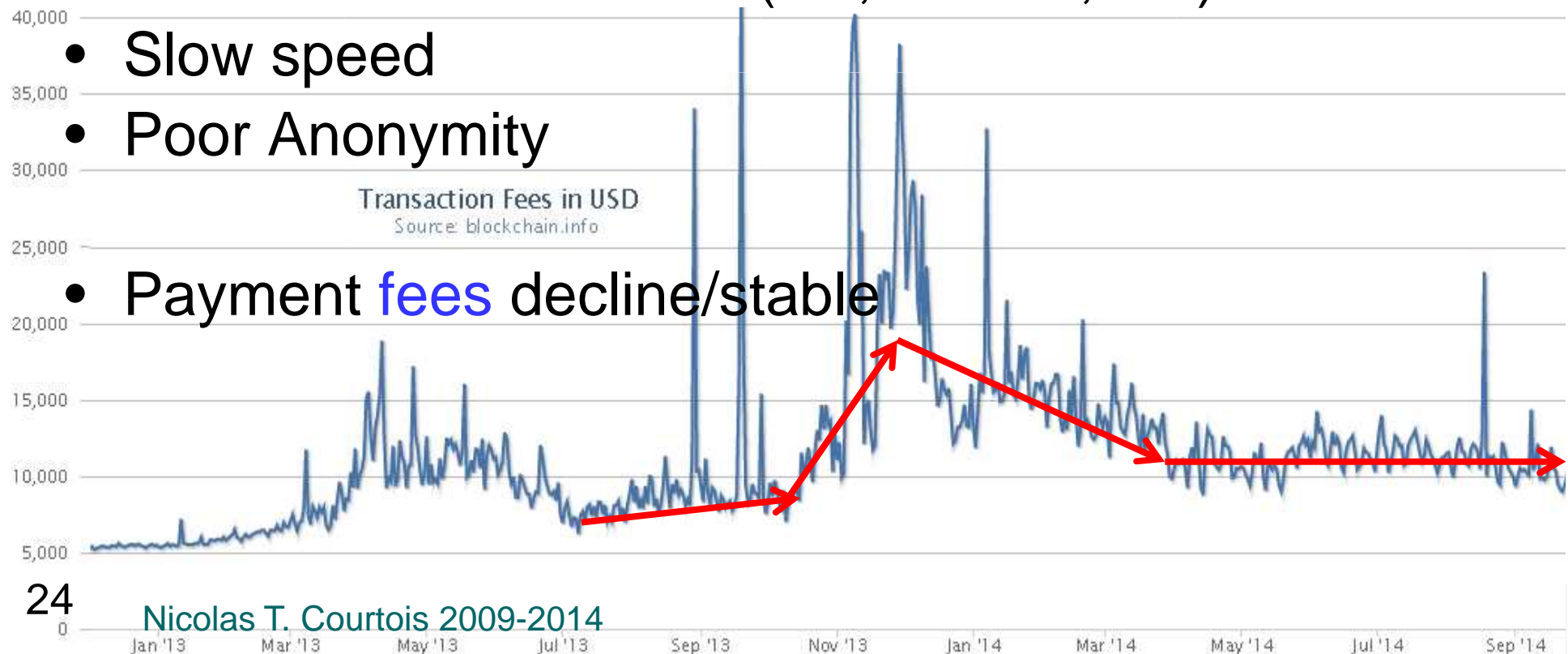
- Don't bet a ridiculous amount!
- As long as we don't have 2000 BTC in this bet, we will simply NOT yet know if bitcoin ECC is broken...

<https://www.betmoose.com/bet/bitcoin-cryptography-broken-in-2015-791>

- Don't expect that code breakers who can make 725,000 \$ elsewhere, will even try to break bitcoin Elliptic Curve
- They would rather steal some bitcoins
 - Possible only if your public key is revealed
 - => Tip: use each Bitcoin address only once!

Bitcoin Troubles

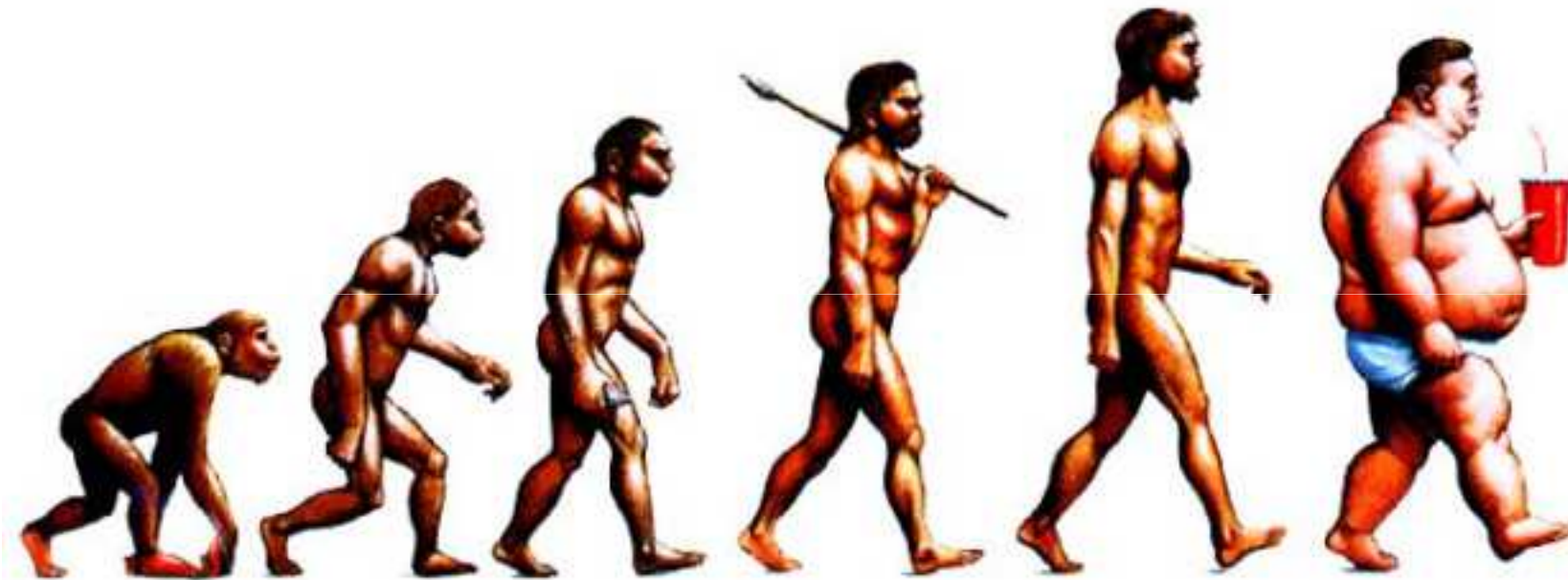
- Crypto gets broken?
- Monetary policy: genius, weird or mad?
- 51% attacks and double spending: easy! ← cf. Levin talk
- P2P network in decline (XX,000=>5,000) ←



So Far...

- Bitcoin has yet failed to achieve the most basic goal: being a decentralized P2P currency

We Need To Do Better!

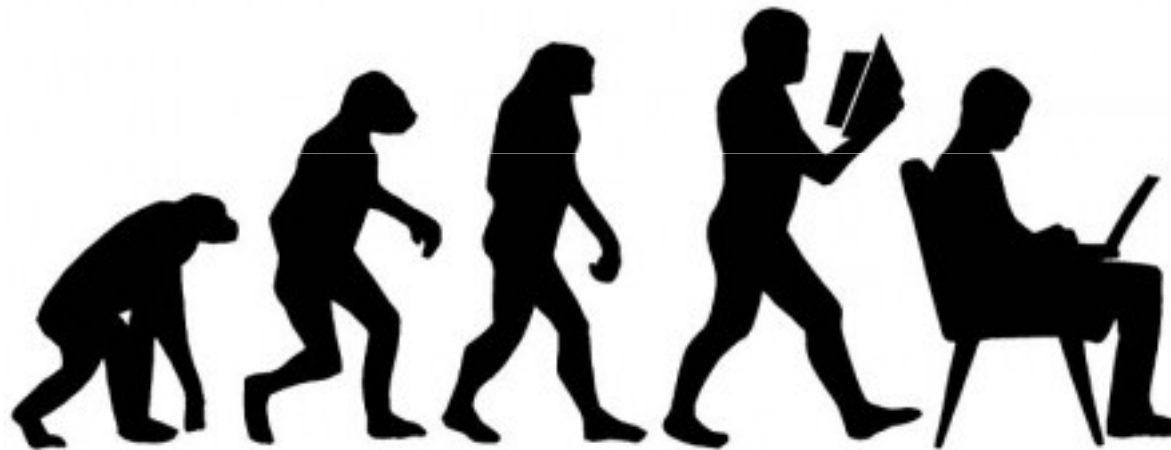


Better?

- The “Yahoo of cryptocurrencies” is now waiting for the “Google of cryptocurrencies” to **steal Bitcoin business** purely on technical superiority and without a single hostile shot.
- This however is NOT guaranteed to happen.

I Was Naïve!

I thought that better security
does automatically happen in the future...



and with more cryptography...

Better Security Will Prevail?

NOT obvious, and **even**
LESS obvious in financial systems.

A right amount of insecurity:

- allows you to sell insurance,
- trains our survival and cybersecurity skills,
- creates lots of interesting jobs for our students,
- possibly avoids criminals to engage in “more violent” crime...

Better “Money” Will Prevail?

Crypto engineers like us
sometimes naively hope that
“better” currencies will drive
“not so good” currencies out of business.

In fact the Gresham-Copernicus Law [1517]
says exactly otherwise!

Bad currencies DO frequently drive better
currencies out of business.

Better “Money” Will Prevail?

The “bad” option is also happening with bitcoin: it has gained excessive popularity

NOT because it was technically very good (it never was) or had solid intrinsic value, or it was fast and convenient (it never was).

It has thrived because it has created huge expectations which temporarily bitcoin competitors could not meet.

Bitcoin remained the obvious choice, a sort of natural monopoly.

Network Effects!

Antonopoulos [former UCL student]

points out that

"when you have a technology that is
'good enough' that achieves network scale [...]
good enough suddenly becomes perfect"

"I don't see any altcoin displacing it", he says.

If bitcoin crashes, again according to Antonopoulos it will
be rather because "we blow it up by accident".

[L.A. Bitcoin Meetup Jan 2014]

Cryptome Renamed My Paper:

CRYPTOME

Donate for the Cryptome Archive of over 81,300 files from June 1996

key. (Local search temporarily disabled, use Google)

Bitcoin: 1P11b3Xkgagzex3fYusVcJ3ZTVsNwwnrBZ

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

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

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





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>
- 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



Need For Speed

<http://video.ft.com/3667480923001/Camp-Alphaville-on-cashless-society/Editors-Choice>,

2 July 2014.

At minute 02.48: Dr. Nicolas Courtois of UCL:

**"[...]It's not true that bitcoin is 'the Internet of Money'.
Bitcoin is 'The Horse Carriage of Money'[...] “**

**“One of the fundamental mistakes of bitcoin is that they use
'the Longest Chain Rule' to decide simultaneously
which block gets accepted and
which transactions get accepted,
[...] a big mistake.”**

Need For Speed – Solutions?



Nicolas Courtois:

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

Nicolas T. Courtois, Pinar Emirdag and Daniel A. Nagy:

Could Bitcoin Transactions Be 100x Faster?

will appear in SECRYPT 2014, 28-30 August 2014, Vienna, Austria.

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

Security => Speed?



Amazing, normally security and speed are opposites.

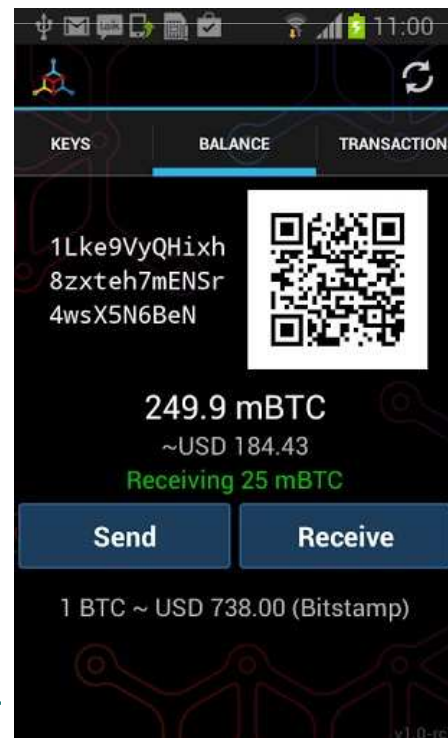
In financial markets one can execute trades microseconds.

In bitcoin we need to wait for **10 minutes** and a large multiple of it for larger transactions.

Speed is **slow mostly out fear of possible double spending** attacks, which imposes certain precautions.

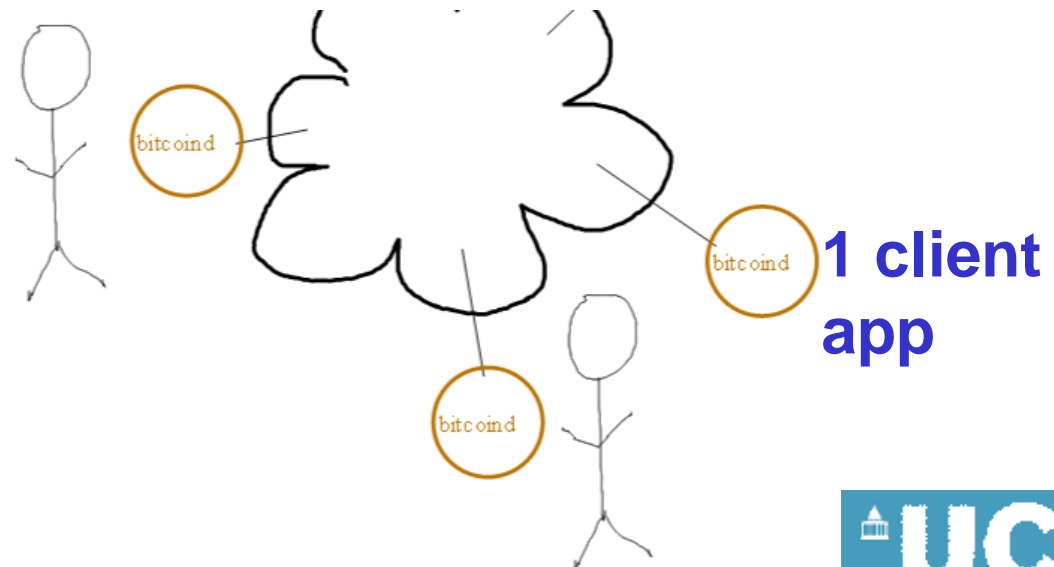
Fixing these security problems
simply allows to make bitcoin transactions
much faster, or rather to **accept them much earlier**.

P2P Payment



Bitcoin Network

- Computers connected into a P2P network...

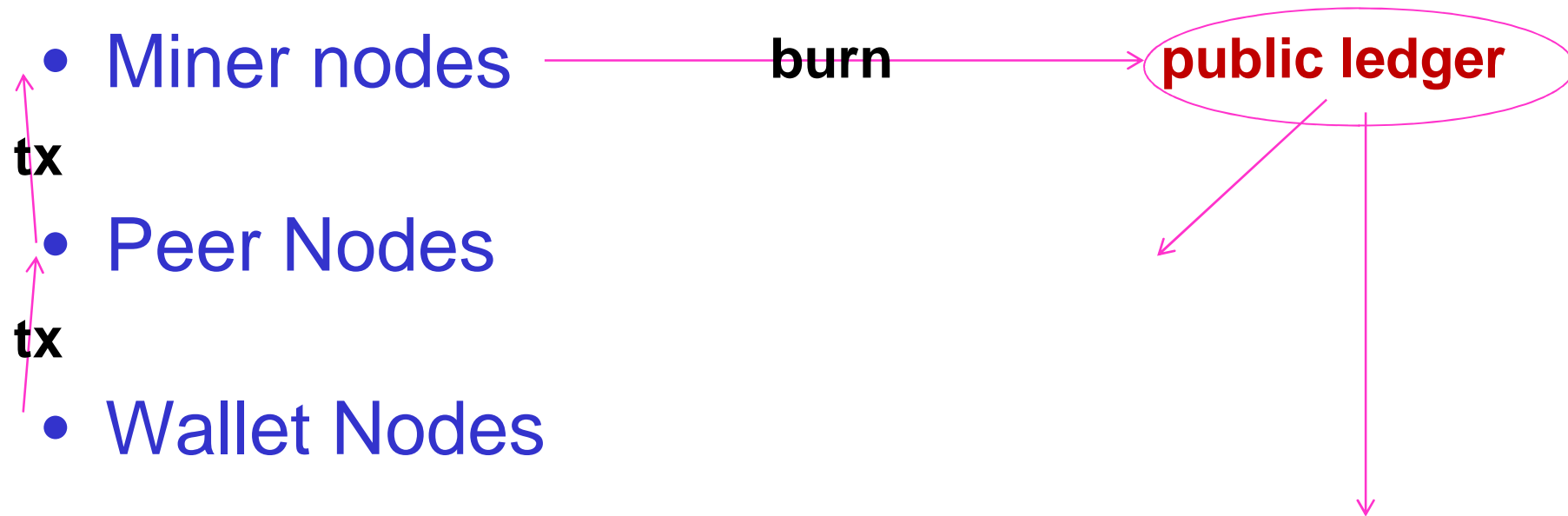




The Reality vs. Satoshi

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

Tx LifeCycle





*Peer Network – Decline

- # active nodes << #miners
- 5K << 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.



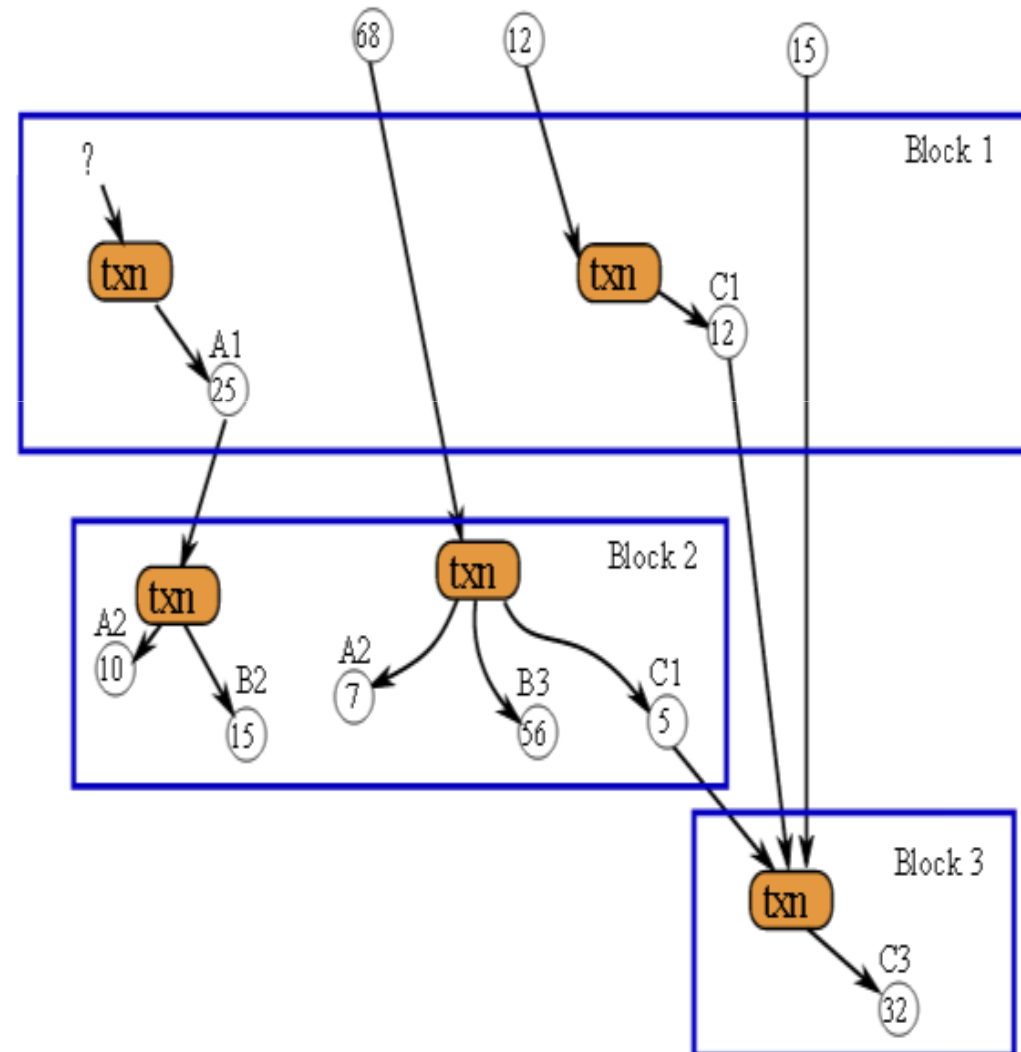
Source: Bitnodes

Block Chain

Def: 
A transaction database

Also a ledger.

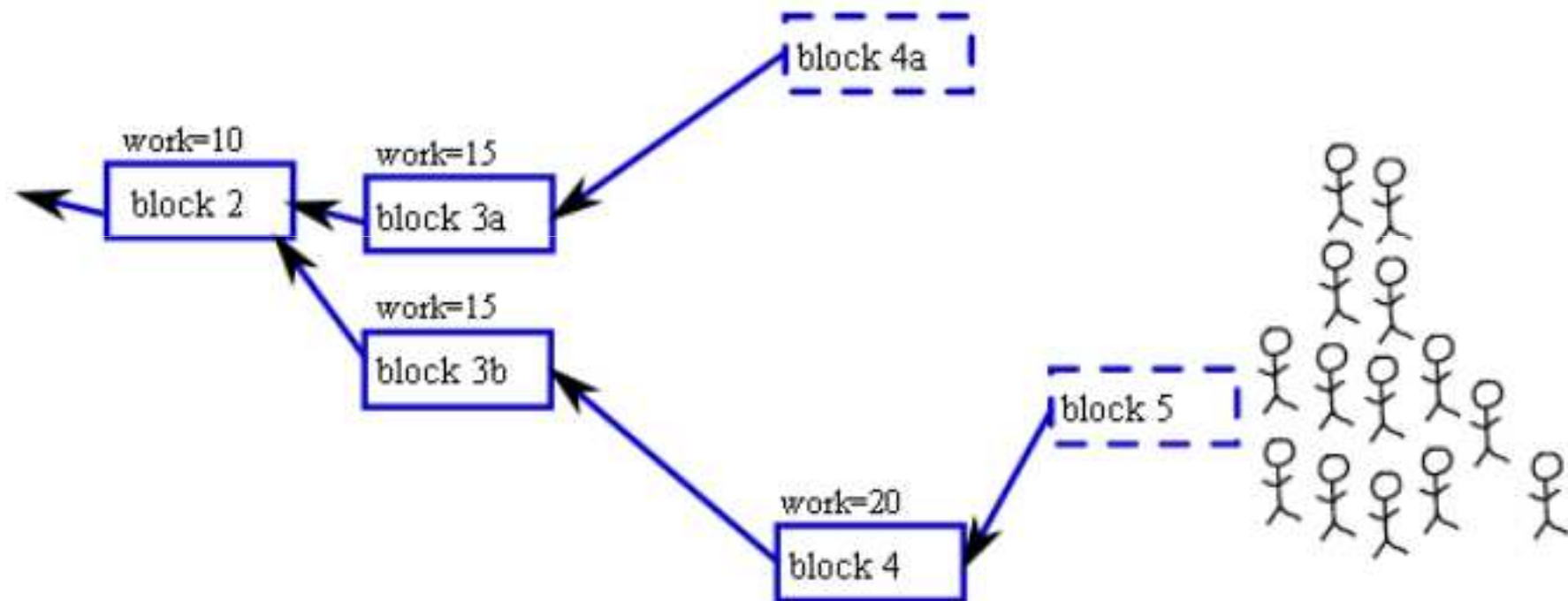
Every transaction
since ever is public.



Longest Chain Rule

[criticised in our paper]

“1 ASIC 1 vote”



Can Sb. Cancel His Transaction?

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

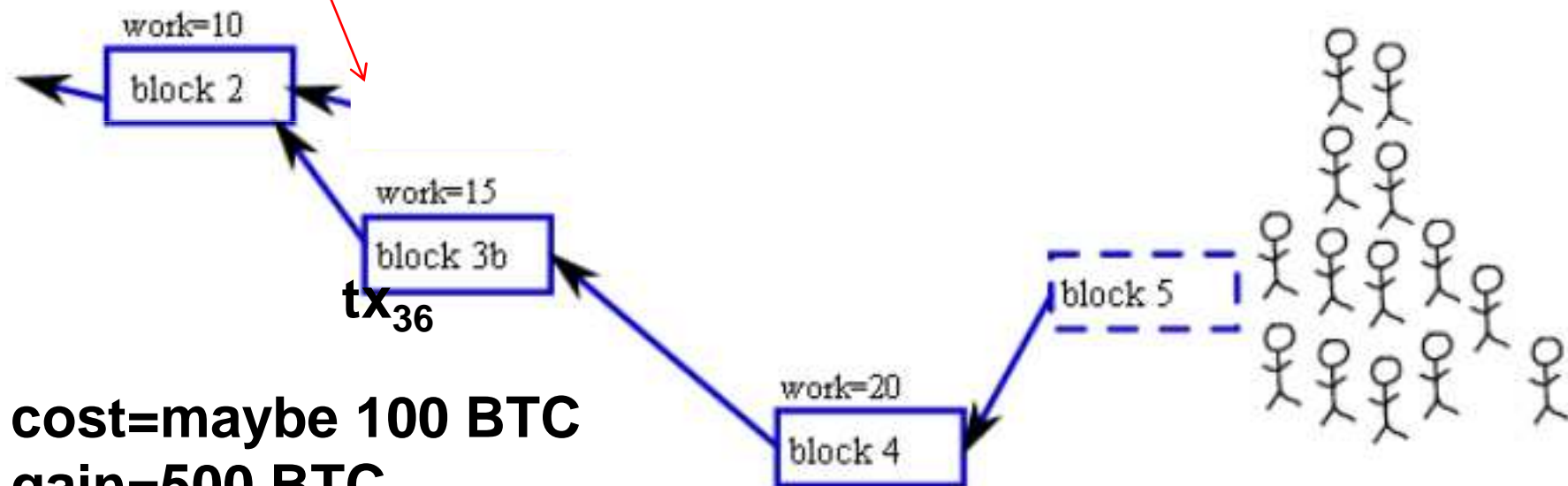
Can be easy or very difficult it depends!



Attack:

Extend This Branch To Cancel One Transaction tx_{36}

Goal: generate 4 blocks.



cost=maybe 100 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:

- devices are privately hold by independent people.

Easy if:

- 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.
- OR if only people mine in pools
 - ⇒ attacks ARE UNLIKELY TO BE DETECTED by miners,

Is it a 51% Attack?

51 % attacks:

almost nobody gets it right ever,

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

Satoshi On 51% Attacks

"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.

He ought to find it more profitable to play by the rules[...] than to undermine the system and the validity of his own wealth."

Satoshi On 51% Attacks

"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.

He ought to find it more profitable to play by the rules[...] than to undermine the system and the validity of his own wealth."

Mistaken: Satoshi failed to see that key problem is the **control**/abuse and NOT ownership of hash power for the purpose of mining blocks, **easier:**

Satoshi On 51% Attacks

"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.

He ought to find it more profitable to play by the rules[...] than to undermine the system and the validity of his own wealth."

Mistaken: Satoshi failed to see that key problem is the **control**/abuse and NOT ownership of hash power for the purpose of mining blocks, **easier:**

- The attacker does not have to be wealthy or powerful.
- **Man in the middle** attackers just need to hack VERY FEW pool manager servers and can abuse the other people's miners.
- In typical mining scenarios the attacker does NOT control the money from mining: the whole process of mining requires exclusively the **public** keys and he does NOT have the **private** keys.
- The honest option does NOT exist

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...

The Question of Dominance

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

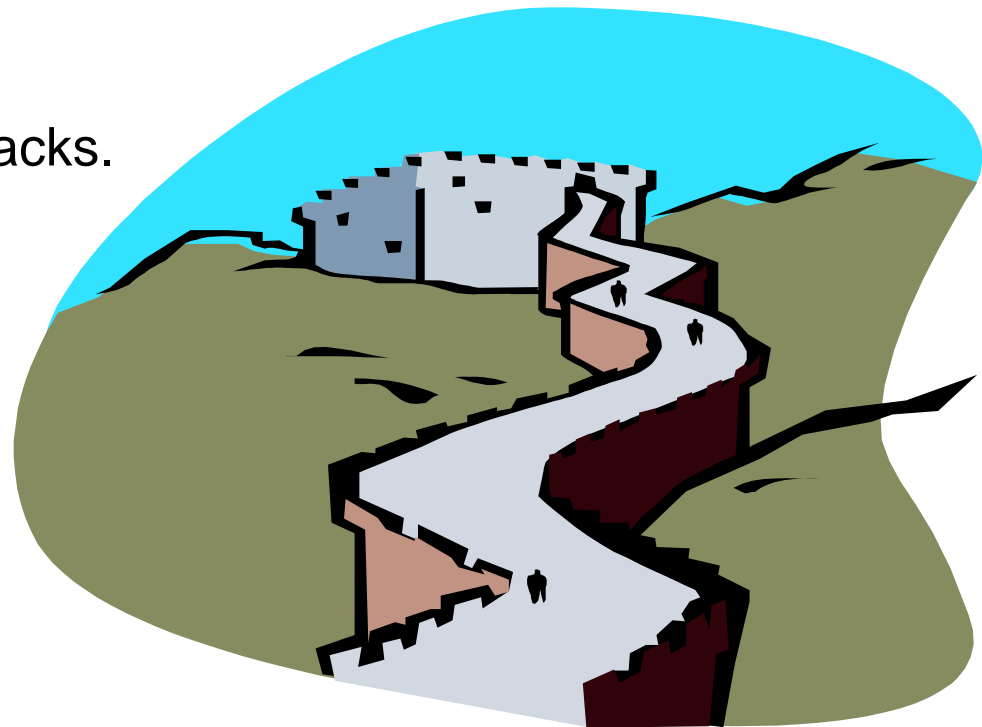
In contrast ALL SMALLER currencies which use a widely used hash function are EXTREMELY EASY to attack

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, [...]"

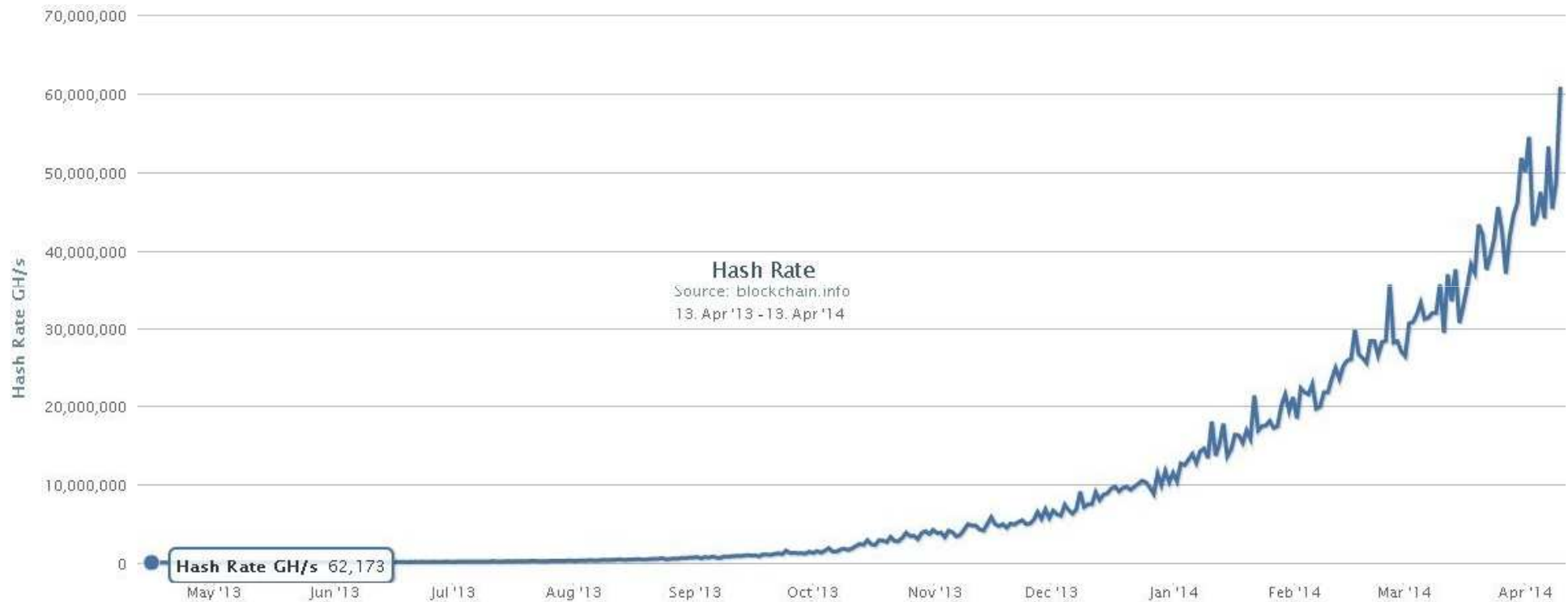
Wow! We have built a "Great Wall".
It protects our money against attacks.

NO THIS IS MISTAKEN



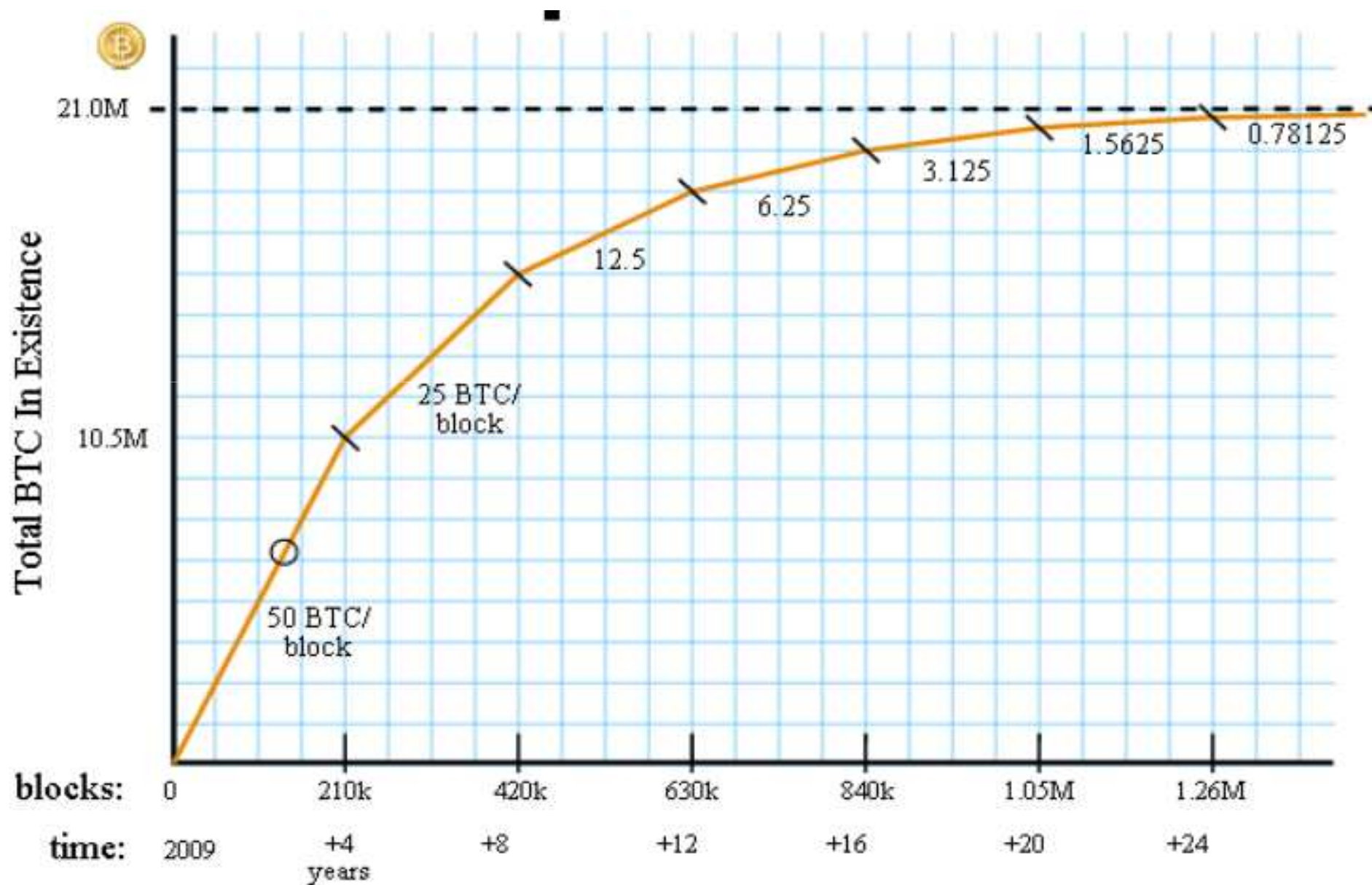
Crazy Hash Power Increase

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



Reward Halving

Built-in Decline



Growth Coins vs. Deflationary Coins

Why Growth Coins Will Win???

Robert Sams: <http://cryptonomics.org/2014/01/15/the-marginal-cost-of-cryptocurrency/>

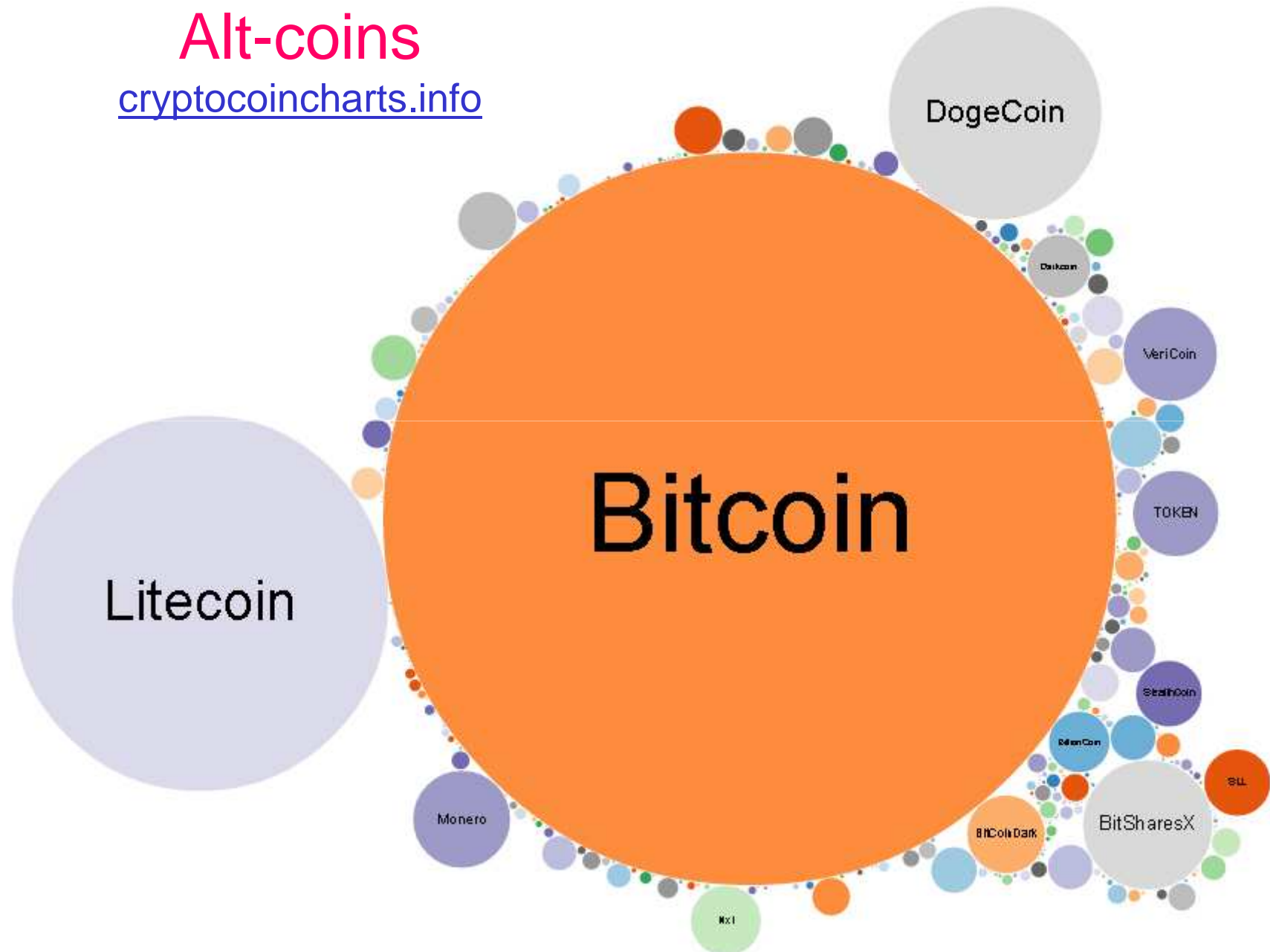
Argument: sooner or later “growth coins” vs. “deflationary currencies” will be in competition.

- little profit will be made by miners who control the network nevertheless
=> they will impose high fees
- thus year after year people will prefer growth coins...

AltCoins

Alt-coins

cryptocoincharts.info



“Stupid Coin” syndrome.

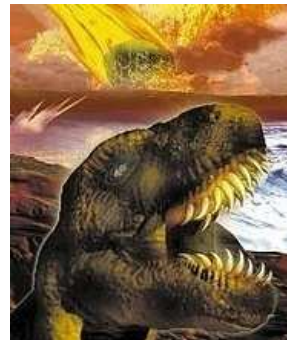
Exact clones are UNBELIEVABLY stupid.

- just stupid copy and paste of open source code
- many are **all broken**: powerful people DO HAVE sufficient computing power to double spend and cheat at any moment...

“Programmed Self-Destruction”

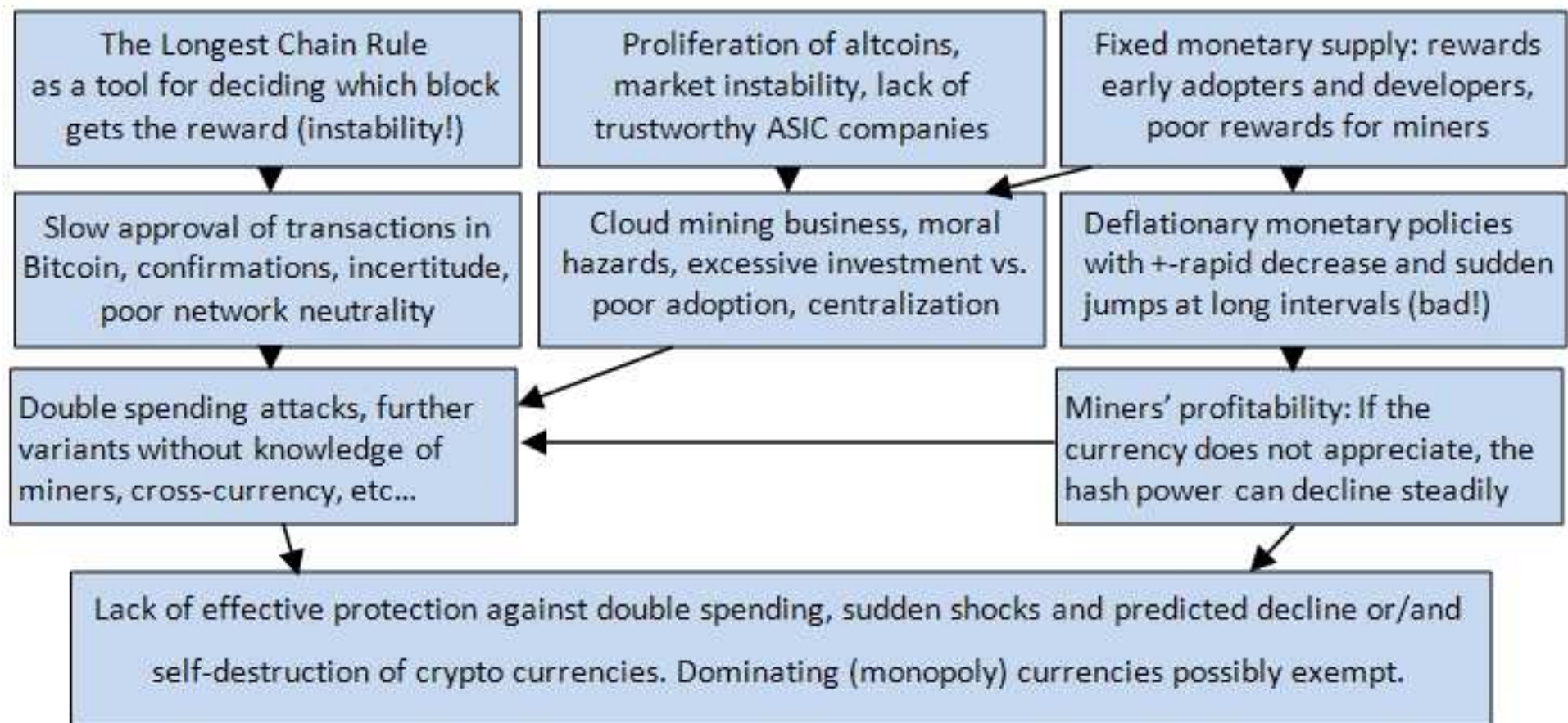
Nicolas Courtois: On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies <http://arxiv.org/abs/1405.0534>

Older version also at <http://cryptome.org/2014/05/bitcoin-suicide.pdf>



Its in the DNA...

Theory of “Programmed Self-Destruction” [Courtois May 2014]



Unobtainium

Unobtanium = UNO – super-rare

unobtanium.io

“The cryptocurrency of serious traders” 😊

Pros:

- SHA256, reuse bitcoin ASICs
- traded at several exchanges
- fast: block = 1.24 minutes
- fixed monetary supply

Unobtanium In Trouble?

- Unobtanium
HUGE PROBLEM!

blocks	approx. dates	UNO/block
1 – 102K	18 Oct 2013-	1
102K – 204K	15 Dec 2013-	0.5
204K – 300K	12 Feb 2014-	0.25
300K – 408K	4 April 2014-	0.125
322,050	-today-	0.125
408K – 510K	5 Jun 2014-	0.0625
510K – 612K	1 Aug 2014-	0.03125
612K –	after 29 Sep 2014	0.0001

Unobtanium In Trouble?

- reward halving every 3 months...
- so what?

HUGE PROBLEM!

smells programmed
self-destruction



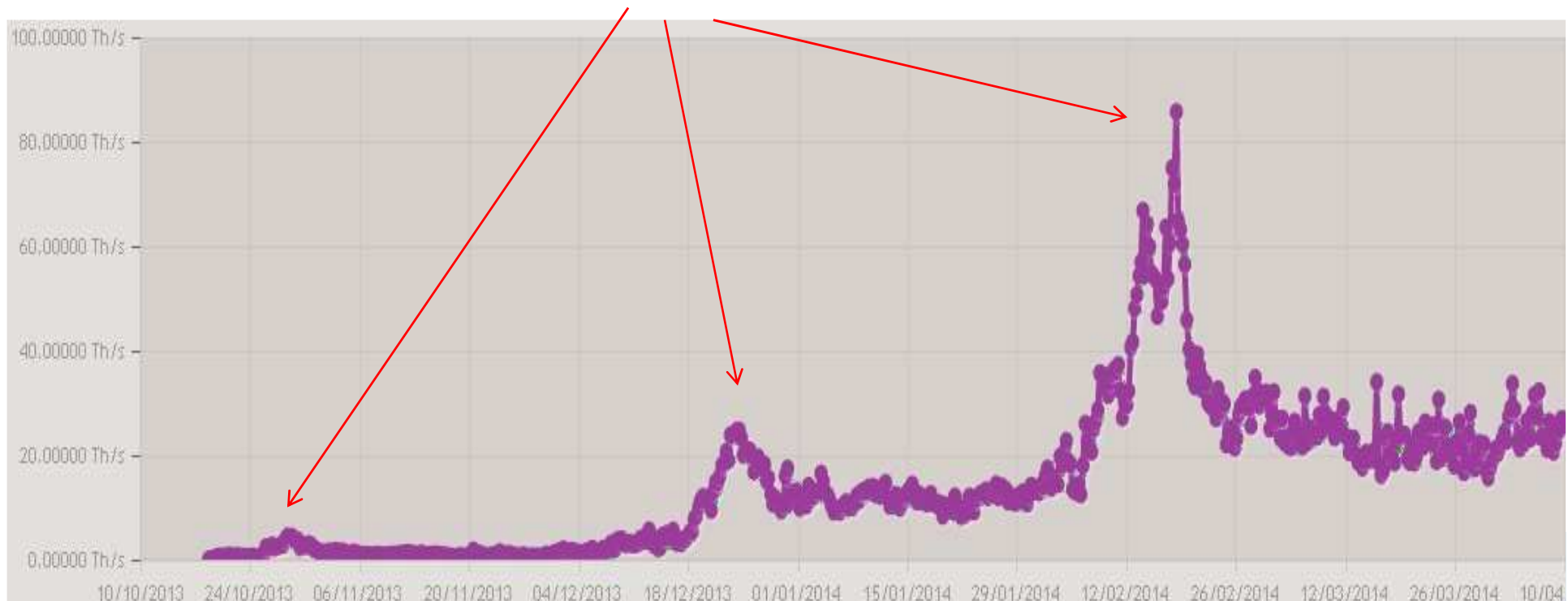
Unobtanium Facts

- 3 months later UNO market price must increase twice OR miners will instantly switch their ASICs to BTC mining... wicked!
- then it must double in the next 3 months...
- Hard to imagine...



Unobtanium Death Warrant

- MAJOR ANOMALY: this currency is already destroying itself!
- miners are already running away from it as fast as they can, WITH SUDDEN JUMPS



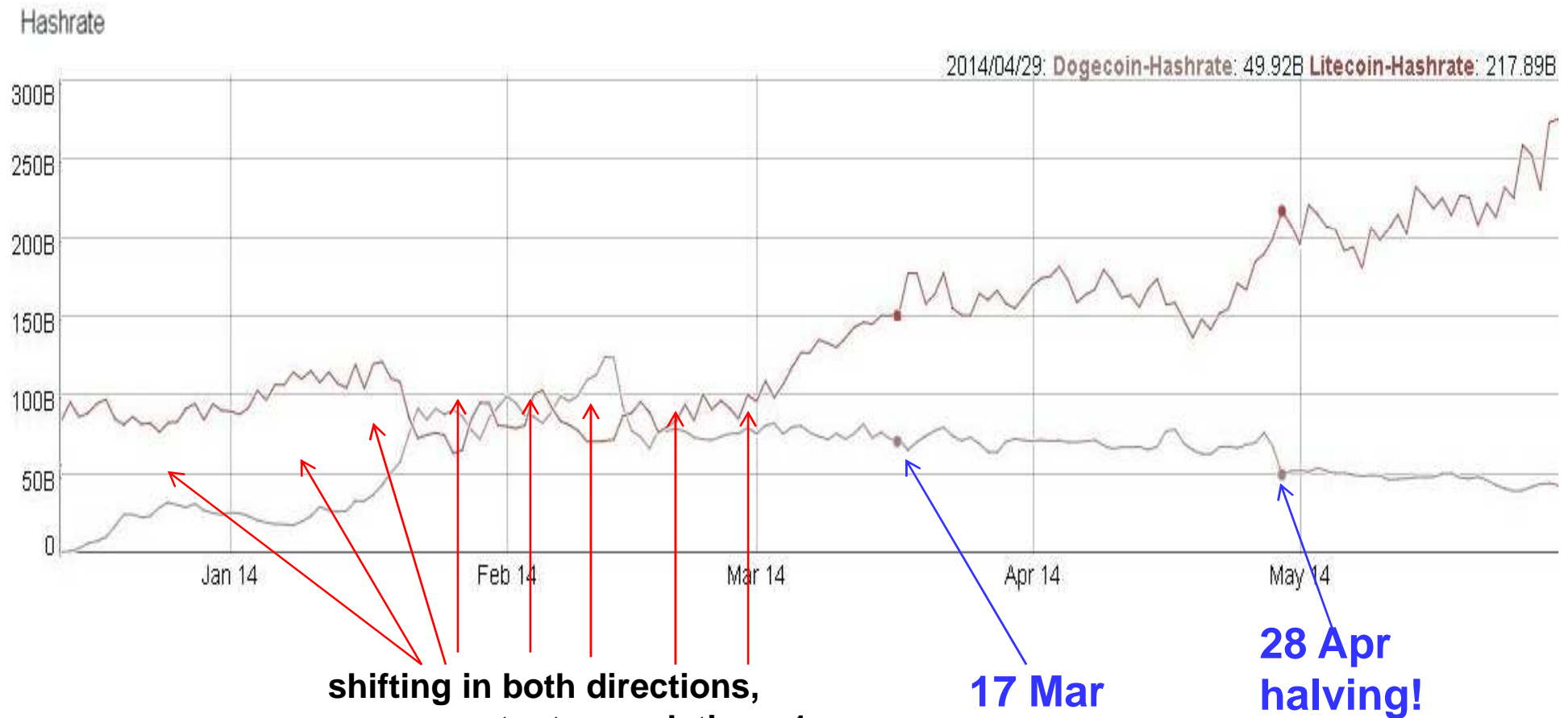
Unobtanium Decline

- My prediction is that the hash power will decline to a ridiculously small value.
- Prediction:
IF the hash rate is maintained,
on 29 Sept 2014 it must achieve $1\text{UNO} = 15,000 \text{ USD}$,
- **A KILL SWITCH**: the reward is DIVIDED 300 times overnight!!!!!!!!!!!!!!!!!!!!!!

DogeCoin Self-Destruction!

DogeCoin Death Warrant

- has seriously challenged LTC, 51% attack was possible in Feb 2014.
- self-inflicted destruction shortly after?



DogeCoin Predicted Decline

- On 28 April:
- One miner was able to execute a double spending attack!



- very bad for DOGEcoin...

Josh Mohland, 4 August 2014

Acknowledged that:

- Dogecoin was never "intended to function as a full-fledged transaction network",
- "Dogecoin was **built to die quickly** –none of us expected it to grow into the **absurd entity** it is today. With that said, there's absolutely an easy way to save the coin from its **certain death** (and by death I mean **51%** attacked [...])"

Way Out!

Merged Mining

VERY GENEROUS:

Litecoin founder Charles Lee
did NOT have to do that.

Like a Bailout!

Bitcoin Monopoly Rents

Accidental, more than deserved.

Programmed self-destruction [cf. our paper]:

- other currencies have copied THESE EXACT mechanisms bitcoin which makes them unable to survive.
- bad for bitcoin clones...
- bitcoin source code was like a VIRUS!

Solutions...

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

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

Ultra Fast Transactions!

Very strange: Satoshi did NOT implement a timestamp for transactions.

Impossible to distinguish between various situations.

Impossible to manage double spending correctly.

- Ask other ordinary peer nodes to confirm your transaction for a fee, within seconds, not a multiple of 10 minutes.
- Chain and mix these confirmations.
- **Accumulate evidence** that one version was propagated much earlier than the other, and accept this version:
 MAKES BITCOIN MUCH FASTER.
 100x speed increase expected.