

Bitcoin Security and Freedom



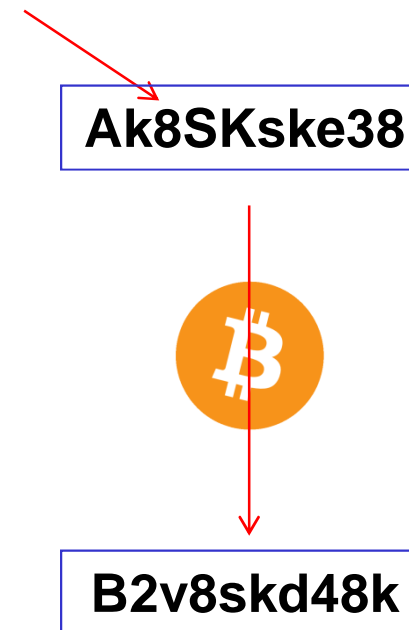
Nicolas T. Courtois

Introducing Bitcoin



Bitcoins

- bitcoins are cryptographic money
 - public ledger: history shows how many bitcoins each user has...
- user has the right to transfer his bitcoins to any other user
 - user are known by their pseudonyms, H(PKeys)
 - each person can use a unlimited number of distinct pseudonyms (accounts)



Digital Signatures

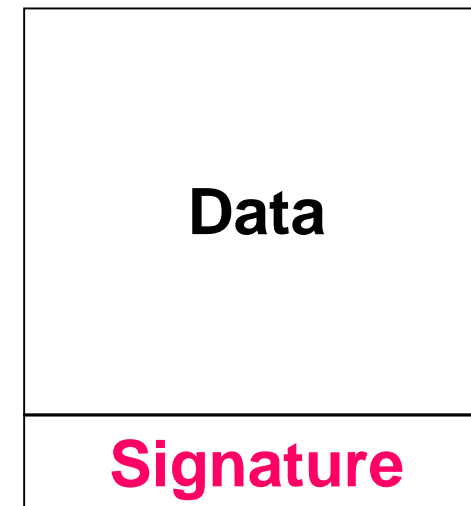


HSBC Holdings plc [GB] <https://www.hsbc.co.uk/>

Attaching a Signature

Signature – def:

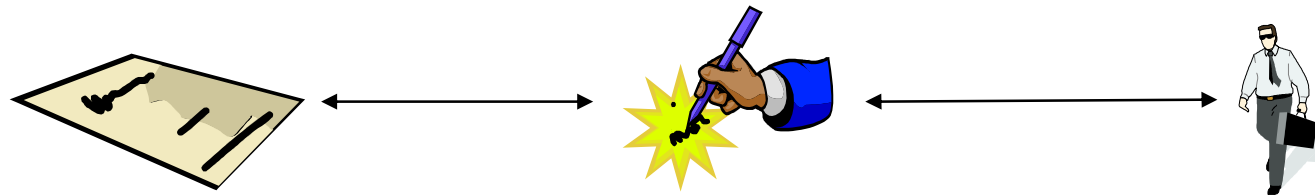
data in **electronic** form which are **attached** to ...
other electronic data
and which serve as a method of authentication.



Signatures

Two main functions

1. Identify the signer
2. Approbation



Digital Signatures

Four main functions total:

1. Identify the signer
2. Approbation
3. **Integrity** of the message
(cannot be modified later)
4. Automatic verification,
+ **Public Verifiability**
(anyone can verify!)

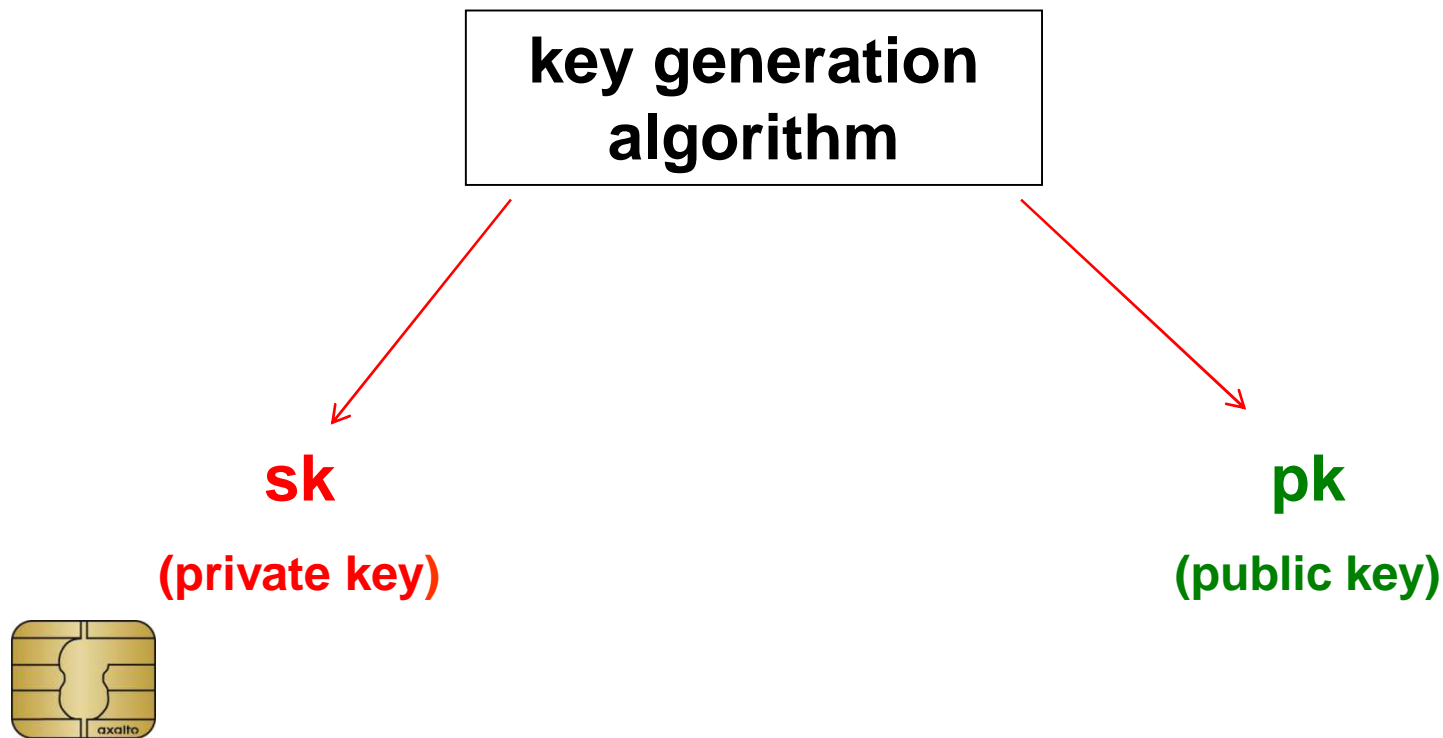


Solutions: Digital Signatures

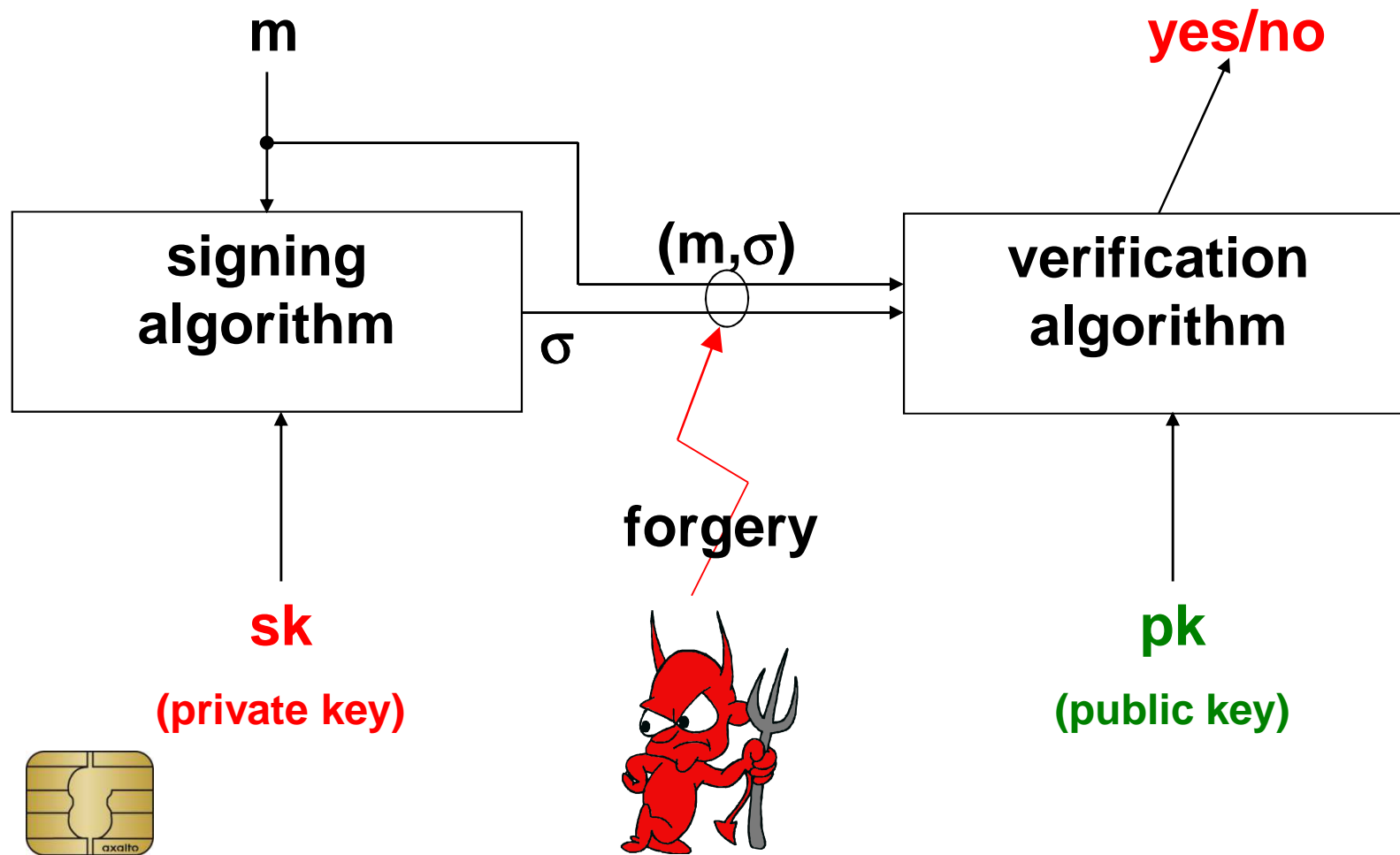


Idea: **cryptographic** solution

Definition: 3 algorithms...



Digital Signature



Bitcoin



New Bitcoins

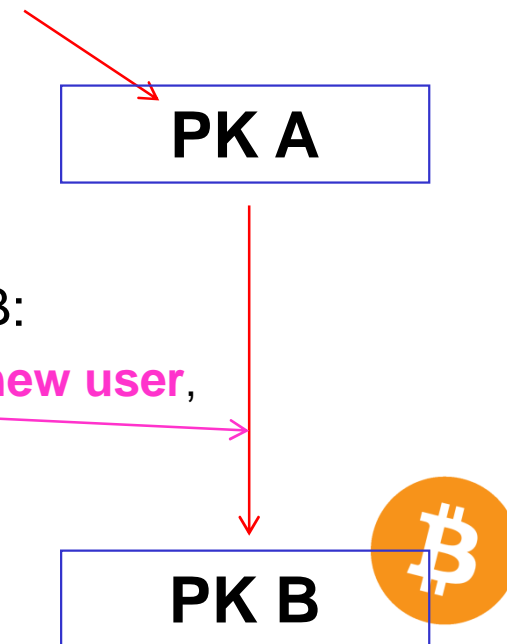
- initially money is attributed through **Proof Of Work (POW)** to one public key A
 - to earn bitcoins one has to “work” (hashing) and consume energy (pay for electricity)
 - do a difficult computation => you have earned 25 bitcoins
 - a sort of lottery, most of the time people team in “pools” and share the gains
 - everybody knows who has these bitcoins: A



Transfer of Bitcoins

- initially money: hard work => public key A

- money transfer from public key A to public key B:
 - simply sign that you transfer the money to a new user,

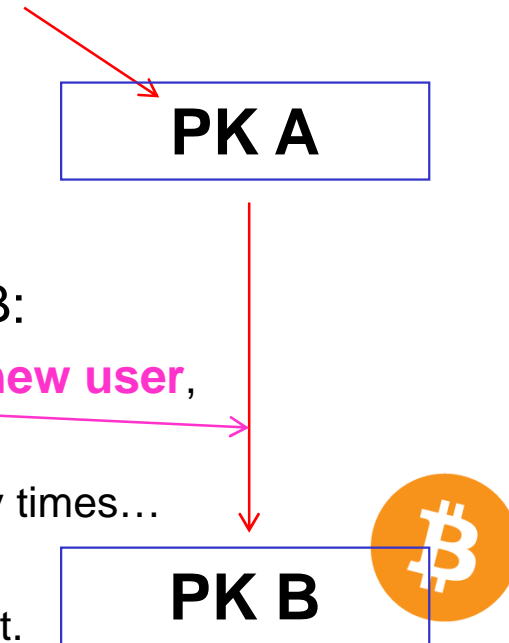


Transfer of Bitcoins

- initially money: hard work => public key A

- money transfer from public key A to public key B:

- simply sign that you transfer the money to a new user,
- multiple confirmations: the network will re-confirm many times...
- we do NOT need to assume that ALL people are honest.
 - with time it becomes too costly to cheat



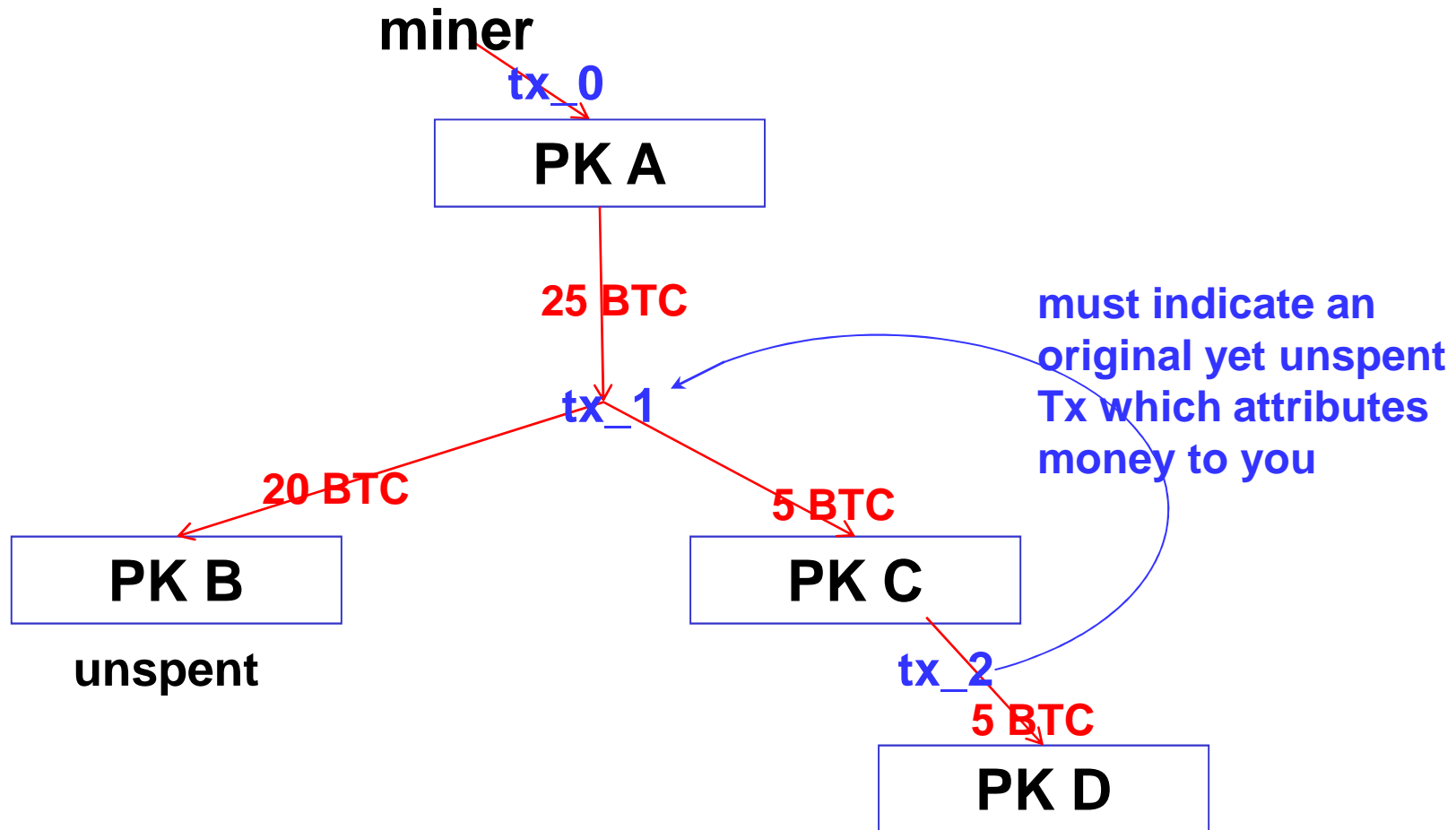


Authorizing Transfer of Bitcoins

- you have a private key => you have the money (right to transfer)
 - keys stored on PCs or mobile phones
 - publicly verifiable, only one entity can sign
- you can transfer ALL yet **unspent** attributions
- if Tx has several inputs
=> everybody must sign
- data to be signed:

<ul style="list-style-type: none">• Origin Tx(s)• Amount(s)• New Owner(s)
Signature

Consecutive Transfers



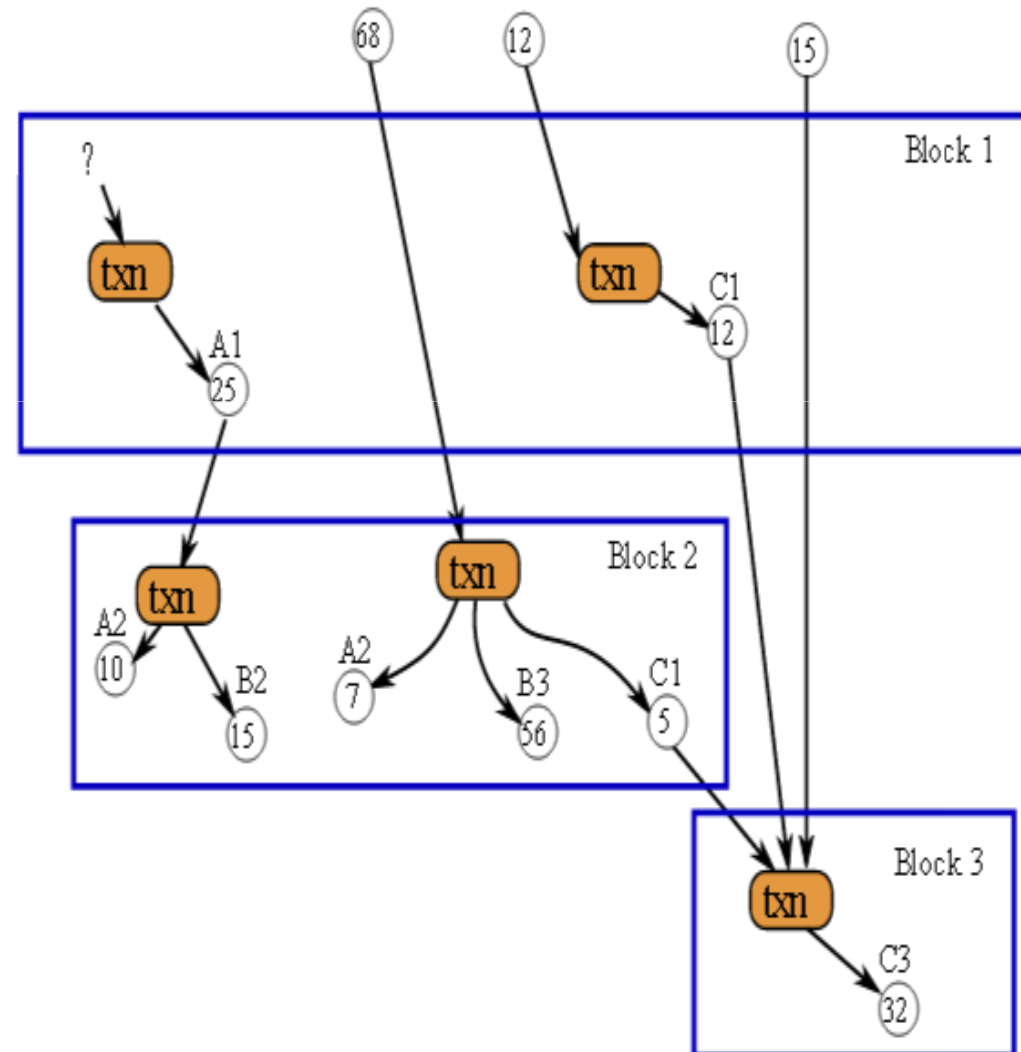
Block Chain

Def: 

Public transaction database
or a ledger.

Every transaction
since ever is public.

Blocks contain a
Proof Of Work (POW)
(they are basically
hard to make)

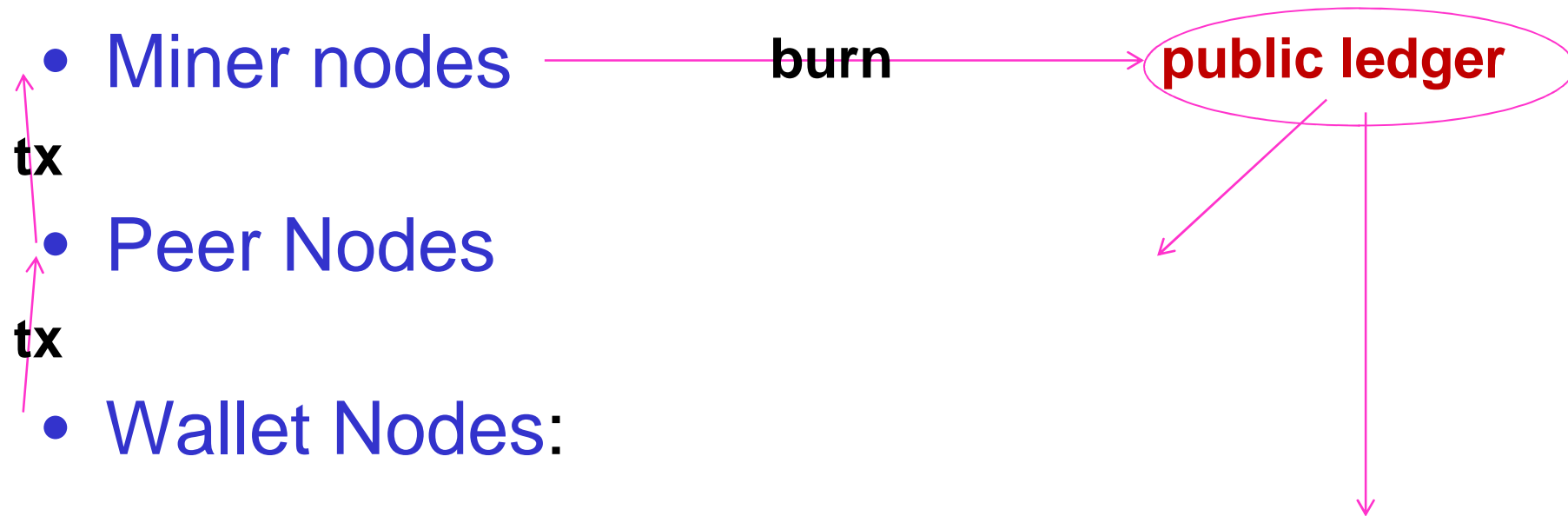


Bitcoin Network

Three sorts of entities:

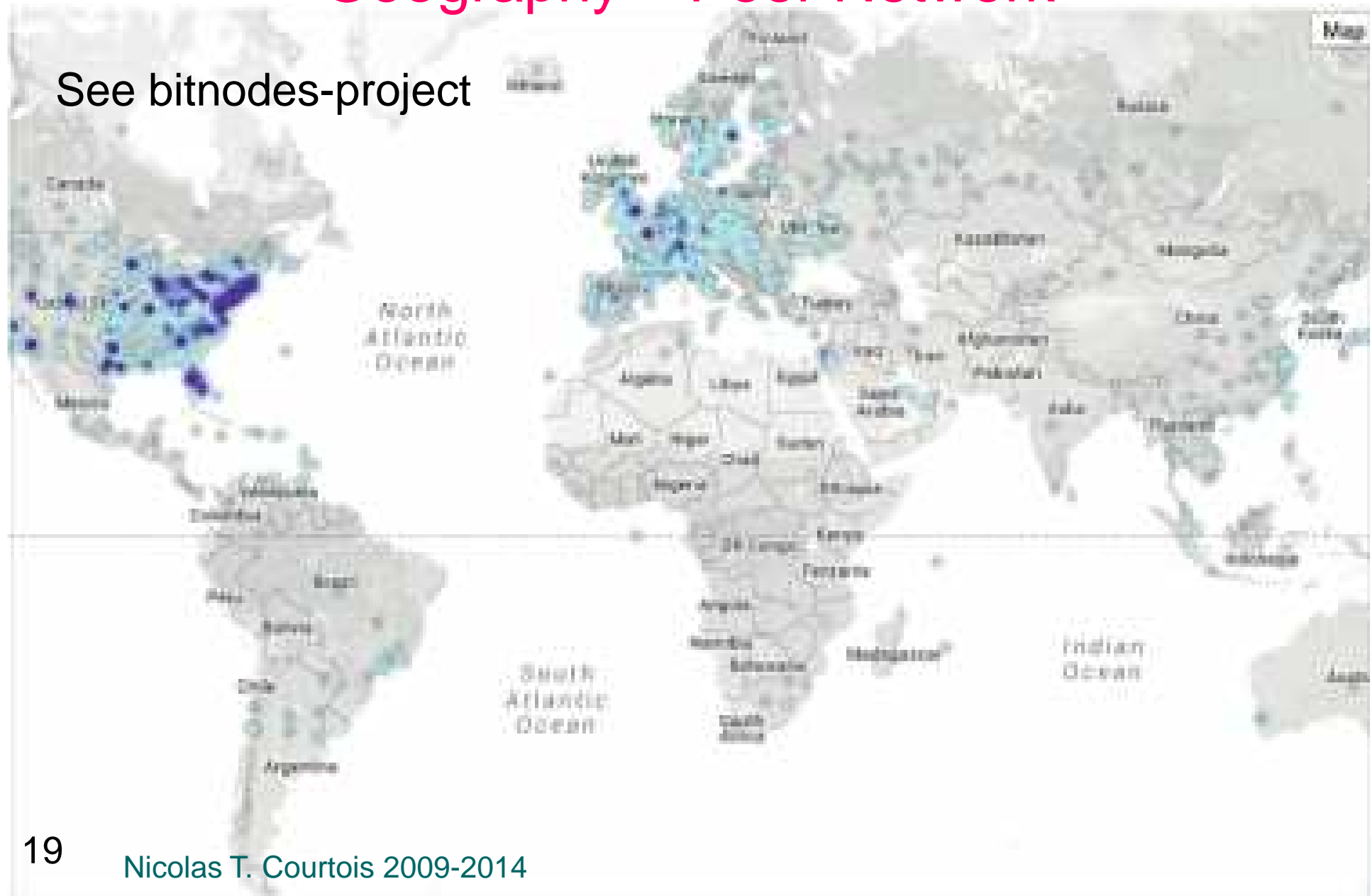
- **Miner nodes** – 50K
 - Hashing with public keys
- **Peer Nodes** – 5K
 - Relay and store transactions and blocks
- **Wallet Nodes** – 5.5M, 0.25M active
 - Store and release funds,
 - Focus on management of private keys, master keys etc etc.

Tx LifeCycle



Geography – Peer Network

See bitnodes-project





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

Are They Crazy?

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

- popularity

legal tender, government standardization and regulation
≤ in Google searches and press/media
bitcoin is a lot more famous than Snowden/NSA etc...

- trust

trustworthy authority
≤ distributed computer system
acting on self-interest
NO NEED TO TRUST ANYONE

Asset Bubble?

In Davos Jan 2014:

“It is a bubble,
there is no question about it.

... It’s just an amazing example of a bubble.”



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



Business Law:

why not 1000% ???

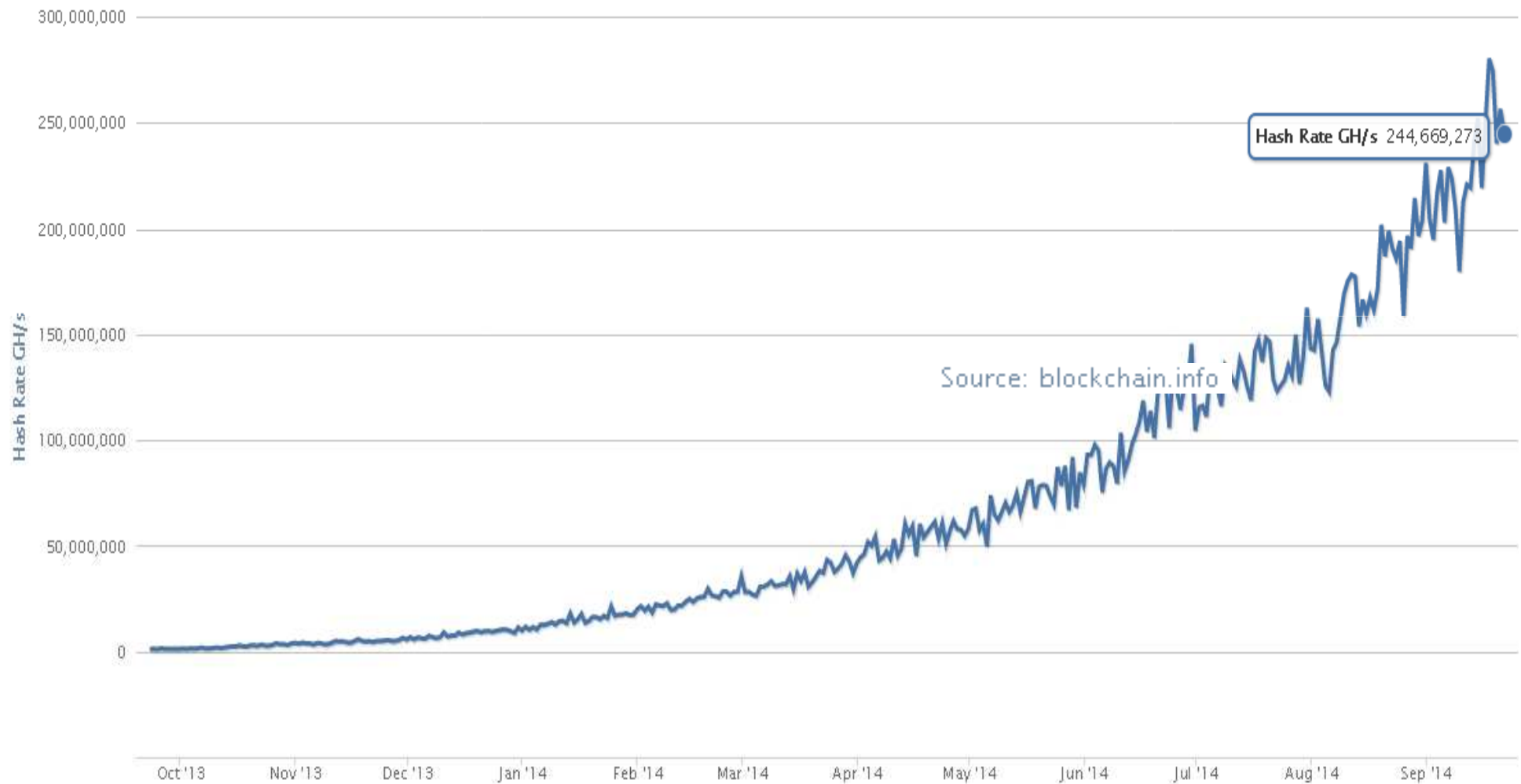


Exceptional High-Tech Industry

Mining energy efficiency has improved the efficiency
10,000 times since Satoshi started mining in early 2009...

Like 1000% per year improvement!

Hash Power: +60% Every Month



Questions:

- How can a community of individuals can run a financial **cooperative** without being manipulated by powerful entities?
- Can we trust the **source code** and cryptography?
- Do we understand the **risks** well enough in order to put our savings in some computer system either private or shared in the cloud?
- The **public authorities** do they need to regulate bitcoin as it was proposed in the New York state?

Trust No One?

We still need to
trust the cryptography
(and cryptographers)



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...
open source which has failed us...



It did NOT help,

The Wolf was allowed to operate



NSA 2013 Budget:

[...] actively engages the US and foreign IT industries to **covertly influence**



Free backups to the cloud

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

Bitcoin



Decentralized peer to peer payment system
based on cryptography

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



Anarchy? Dark Side

- In Bitcoin many things which are BUGS are presented as FEATURES:
 - monetary policy (or the lack of one) – frequent criticism
 - problematic cryptography=
 - anonymous founder syndrome, standardized yet TOTALLY disjoint from normal industrial cryptography, NOBUS syndrome (NSA jargon)
 - decision mechanisms (the Longest Chain Rule)
 - no reason why the same mechanism decides which blocks are valid and which transactions are valid, by far too slow, too unstable, too easy to manipulate
 - 51% attacks ARE realistic feasible and ... INEXPENSIVE!
 - sudden jumps in monetary policy => genetically-programmed self-destruction of many crypto currencies
- See: 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>



Dangers of Open Source

- the open-source nature of the developer population provides **opportunities for frivolous or criminal behavior** that can damage the participants in the same way that investors can be misled by promises of get rich quick schemes [...]
- one of the biggest **risks** that we face as a society in the digital age [...] is the **quality of the code** that will be used to run our lives.

Cf. Vivian A. Maese: [Divining the Regulatory Future of Illegitimate Cryptocurrencies](#), In Wall Street Lawyer, Vol. 18 Issue 5, May 2014.

Citation

Bitcoin is:

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

Improve Quality/Security?

Bitcoin Has The Solution!

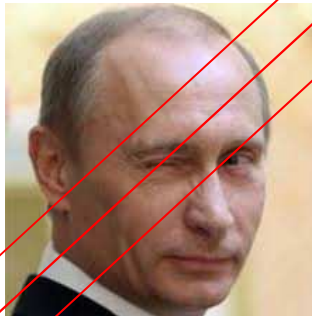


Future belongs to

self-funded open-source communities

⇒ can hire programmers, security experts, etc...

⇒ avoid code of dubious origin



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

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



Timely Denial

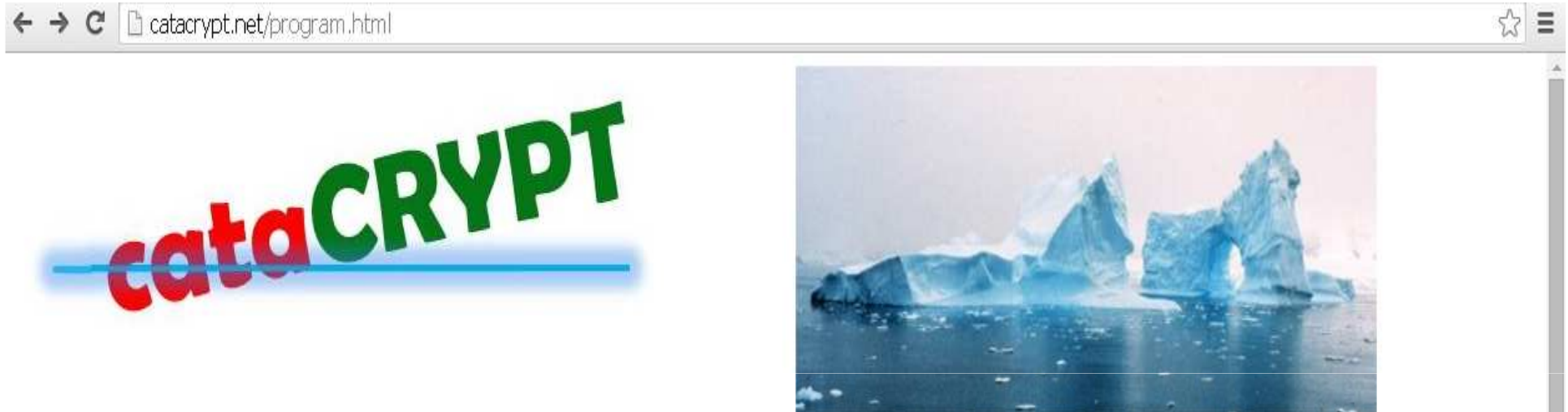
Dan Brown, chair of SEC [Certicom, Entrust, Fujitsu, Visa International...]

"I am surprised to see anybody use secp256k1"

September 2013,

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

What If? CataCrypt Conference



Workshop on **cata**strophic events related to **crypt**ography and their possible solutions

Technical Program

[Home](#)

[Committees](#)

[Call for contributions](#)

[Program \(schedule\)](#)

	Venue: Grand Hyatt San Francisco, Union Square, 345 Stockton Street, downtown San Francisco: room Fillmore A - Theatre Level http://grandsanfrancisco.hyatt.com October 29, 2014 (together with IEEE Conference on Communications and Network Security (CNS))
08:15 – 08:25	Opening Remarks: Jean-Jacques Quisquater (UCL, Belgium)



Wanna Bet?

Bitcoin Cryptography Broken in 2015

Category: [Bitcoin](#)

By  [NCourtois](#) ★★★★★

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 - Totally Anonymous Bets In BTC!

FEATURED

Bitcoin Cryptography Broken in 2015

Category: Bitcoin By  NCourtois ★★★★★

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.

YES

Volume:	₿ 0.140
# of Bets:	3

₿

PAYOUT	ROI
₿ 0.00	0%

* assumes current weight and volumes

Place Anonymously

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!

Solutions

- Use each fresh bitcoin account only once!
- Satoshi did sth really brilliant:
 - Most transactions **do NOT reveal the public key**.
 - full disclosure is unbelievably stupid and simply BAD security engineering and BAD security management.
 - Example:
 - ATMs top-level public keys

Freedom

Hegel [1770-1831], German philosophy

The history
is the process
of broadening
freedom.

For Years I Thought That..

Freedom $\rightarrow \infty$

\Rightarrow

Security $\rightarrow 0$

Freedom \Rightarrow Security issues...

Examples:

- invention of train
 \Rightarrow pickpockets
- car traffic:
 \Rightarrow major cause of death (2M/year)
- invention of the internet
 \Rightarrow pirates and hackers

I was WRONG!

Freedom and Security
CAN co-exist!

I Also Always Thought That..

Speed $\rightarrow \infty$

\Rightarrow

Security $\rightarrow 0$

We Can Have (At Least Sometimes)

Freedom $\rightarrow \infty$

Speed $\rightarrow \infty$

Security $\rightarrow \infty$



Good news AD2014:

MultiSig, SideChains



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**.

Freedom - 1989



9 Nov 1989 Berlin Wall Has Fallen



In Eastern Germany

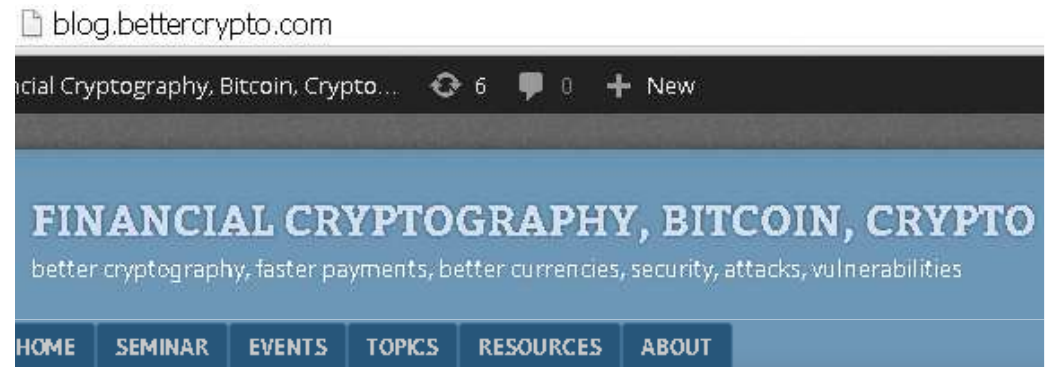
Individuals could NOT
own a typewriter,
or a photocopier,

=> required a permission
from the government!



Today

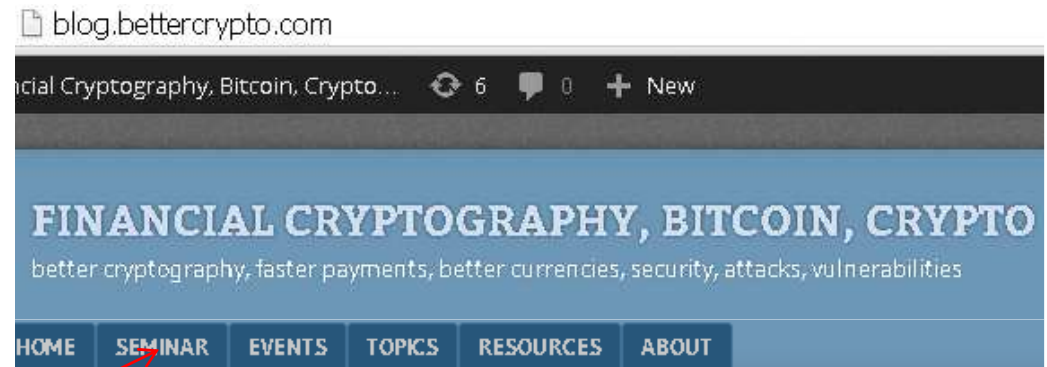
- anyone can have a blog.



New Powerful Attacks On ECDSA In Bitcoin Sys

Today

- anyone can have a blog.

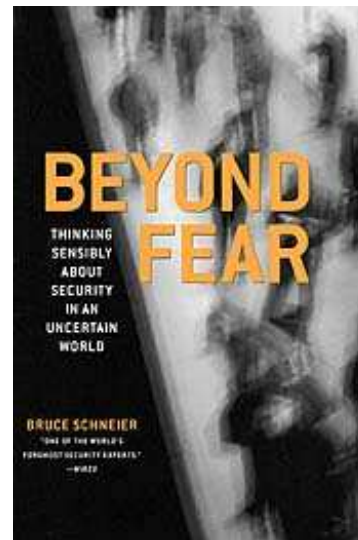


New Powerful Attacks On ECDSA In Bitcoin Sys

UCL Bitcoin Seminar

(runs every week, more or less)

Freedom vs. Security



Sacrifice Freedom?

“They that give up essential liberty
to obtain a little temporary safety
deserve neither liberty nor safety.”



Benjamin Franklin,

engraved on the base
of the Statue of Liberty

We failed to protect our DATA



We failed to protect our **MONEY**



Wind of Freedom

In theory,

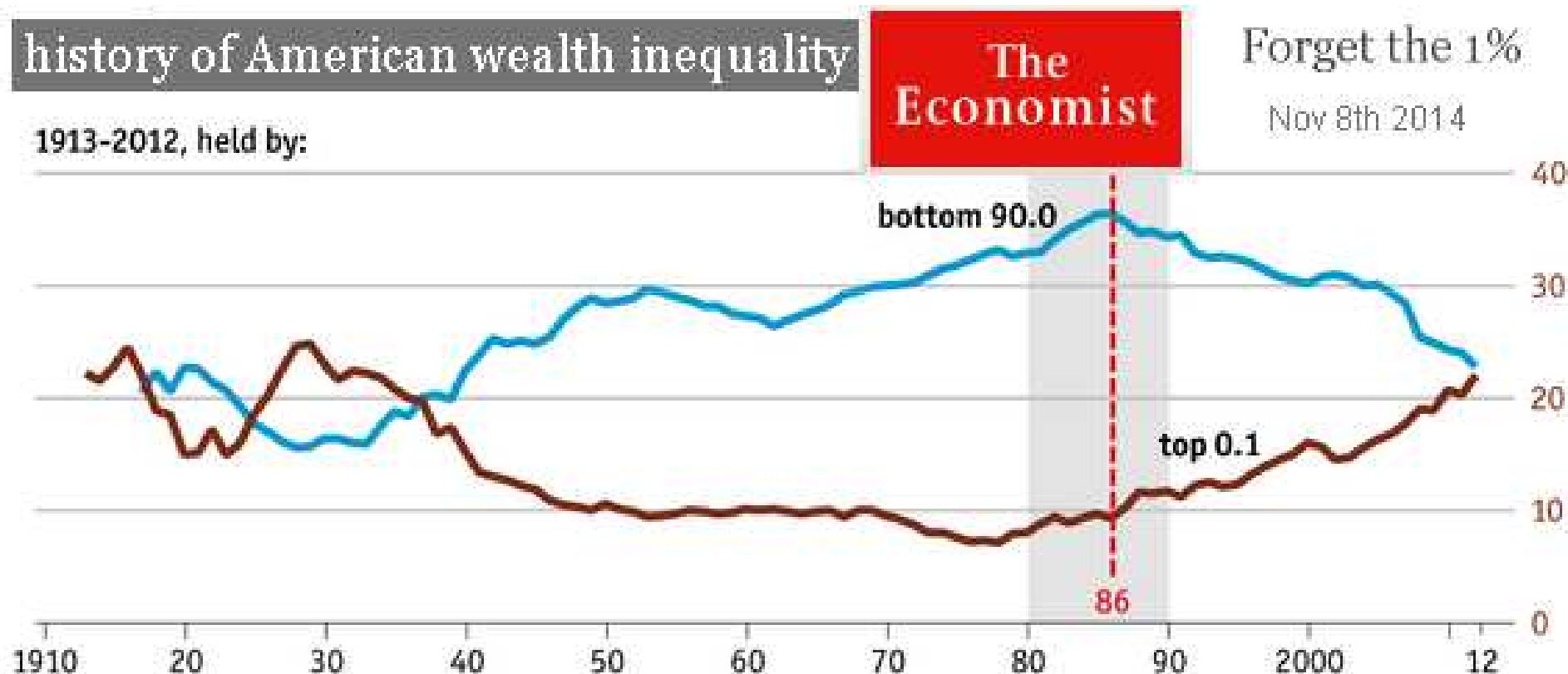
- bitcoin promises to end up the sordid monopoly of bankers to govern our lives and our money



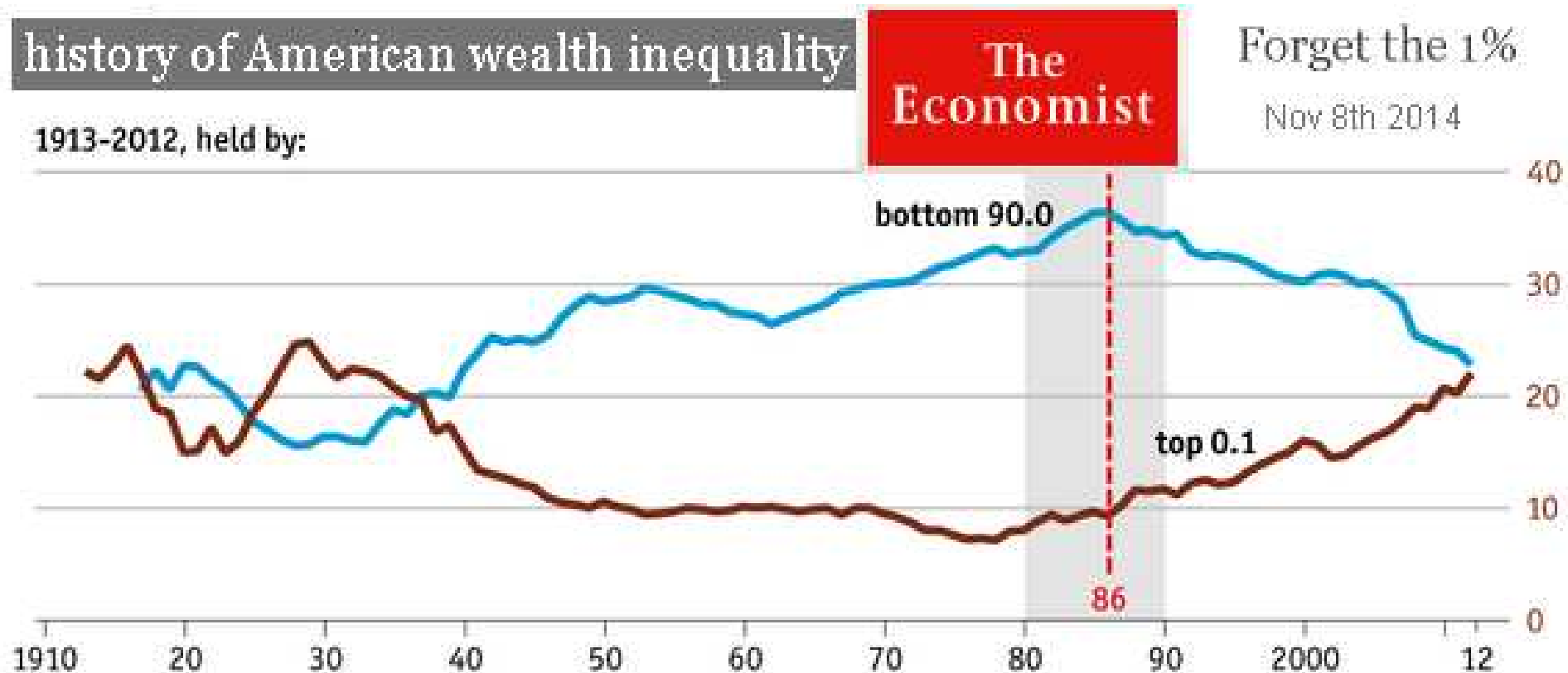
In practice:

- freedom is always eroded if we don't fight for it
e.g. centralization of bitcoin, 51%, etc.

In the Last 25 years Freedoms Have Declined!



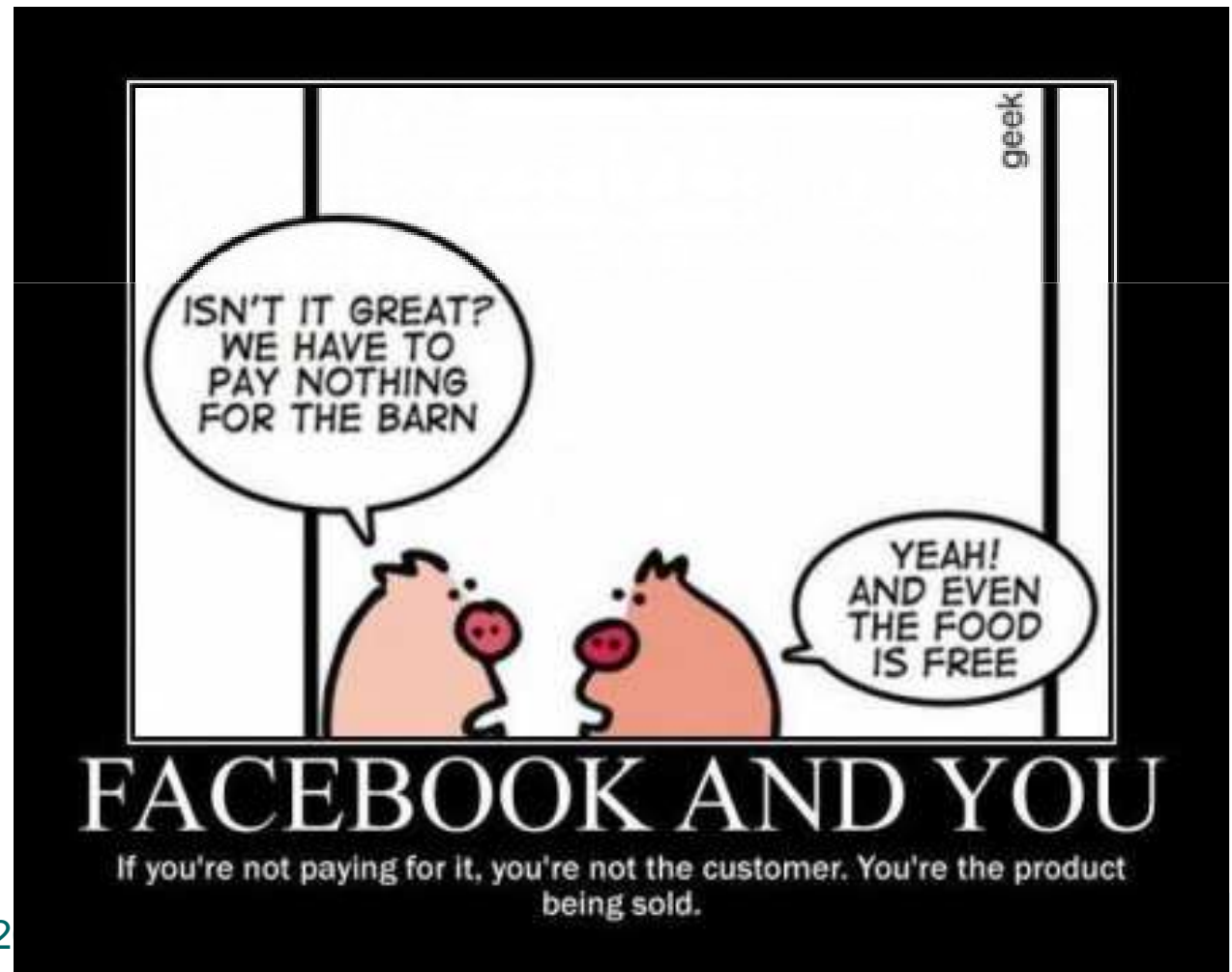
In the Last 25 years Freedoms Have Declined!



Physical Oppression => Financial Oppression

Key Problem:

After few brief episodes of capitalism,
modern business favours slavery.





debt

**fake
competitive
markets**

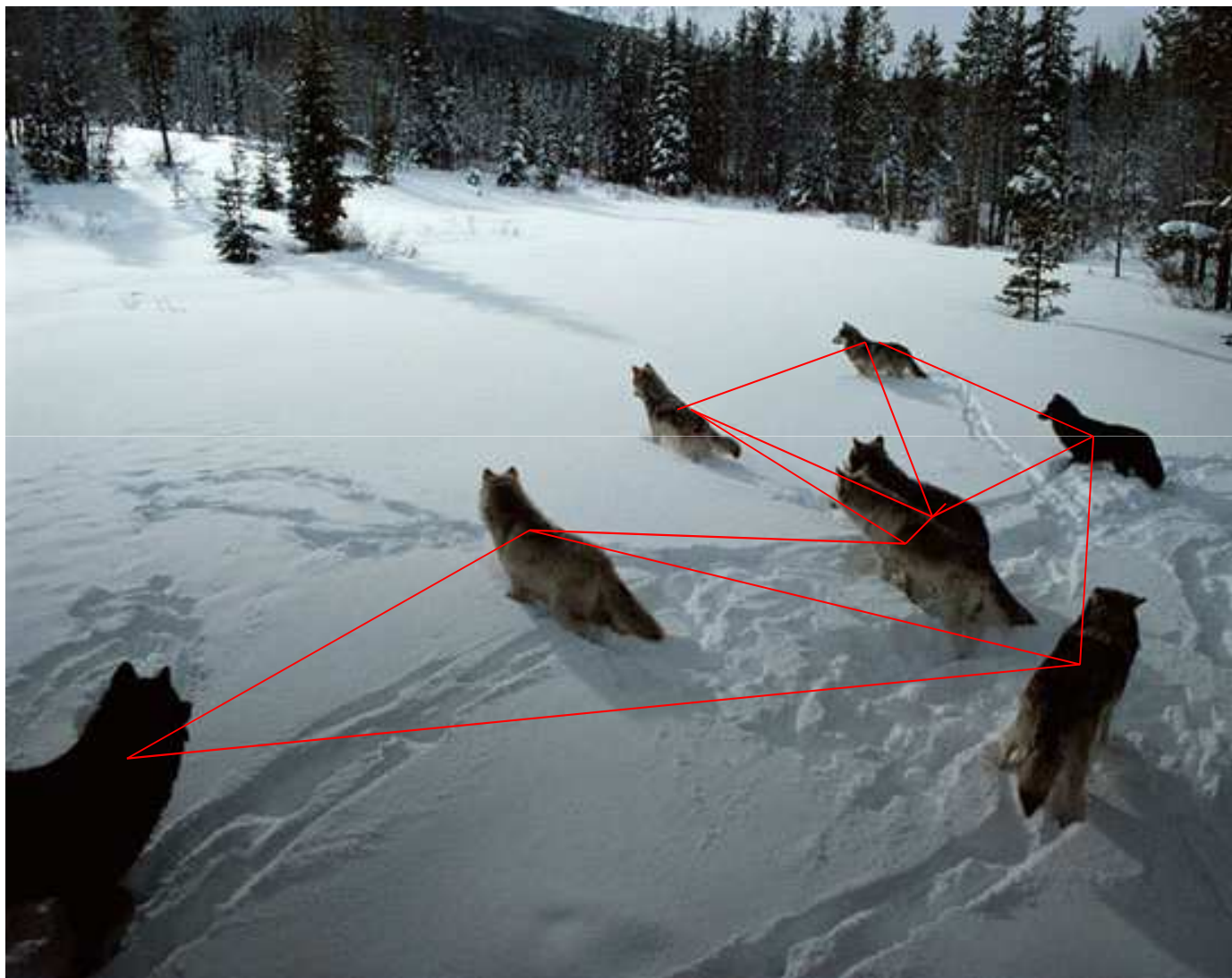
acquire a customer and treat
him like a piece of s**t

More Slavery

**robots
computers
algorithms**



Solution = Decentralization



Miracle Of Bitcoin



Removes two pillars of money:

- “trust”

=> P2P self-regulation
based on self-interest?

- legal/government protection and policing

=> anarchy!



Decentralized P2P Finance



- 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?
 - ...
- Now we have a small piece of [...] code that will allow people to solve [...] problems without reference to “the authorities”.

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

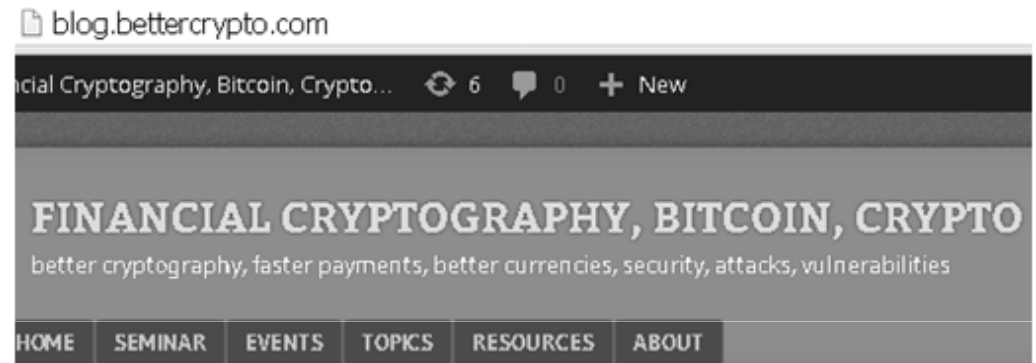
[11 June 2014]

The Telegraph

The coming digital anarchy

20th Century

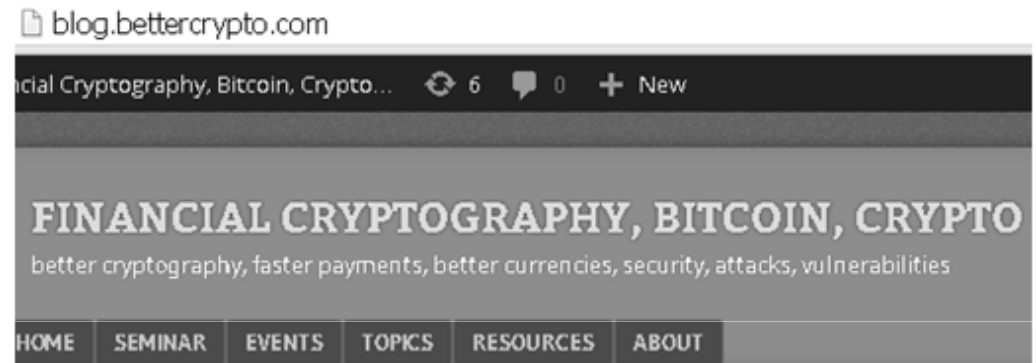
- anyone could have a blog...



New Powerful Attacks On ECDSA In Bitcoin Sys

21st Century:

- anyone could have a blog...



New Powerful Attacks On ECDSA In Bitcoin Sys

- anyone can print his own currency!



*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
- money cannot be confiscated [cf. Cyprus banks].
- it forces finance to become more “transparent”

Ban Bitcoin?



Ban Bitcoin?

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



Krugman

- Bitcoin is ...
 - “the anti-social network”
 - “bitcoin is evil”
- 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