Bitcoin Madness for Cryptographers

(survey and work in progress)

Nicolas T. Courtois [1]

Jean-Jacques Quisquater [2]

[1] - University College London, UK

[2] - Université Catholique de Louvain, Belgium

Our Works on Bitcoin

-cf. also blog.bettercrypto.com

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

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

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

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

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

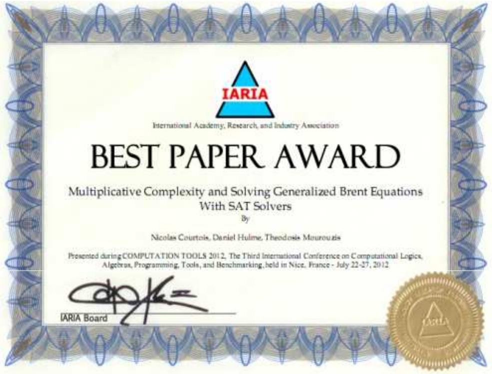
-Nicolas T. Courtois, Pinar Emirdag and Filippo Valsorda: Private Key Recovery Combination Attacks: On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events, 16 Oct 2014, http://eprint.iacr.org/2014/848

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

-New paper: see last slide…

Dr. Nicolas T. Courtois

1. cryptologist and codebreaker



IARIA

International Academy, Research, and Industry Association

BEST PAPER AWARD

Multiplicative Complexity and Solving Generalized Brent Equations With SAT Solvers

By

Nicolas Courtois, Daniel Hulme, Theodosis Mourouzis

Presented during COMPUTATION TOOLS 2012, The Third International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking, held in Nice, France - July 22-27, 2012

IARIA Board

NewScientist
The global science and technology weekly | 7 June 2003
NEW! US JOBS SECTION
MEGAWATER
The biggest engineering folly of all time?
JOHN BARROW
How our world could be just a computer simulation
CIPHER CRISIS

UNIVERSITY CIPHER CHAMPION

March 2013

Cyber Security Challenge UK

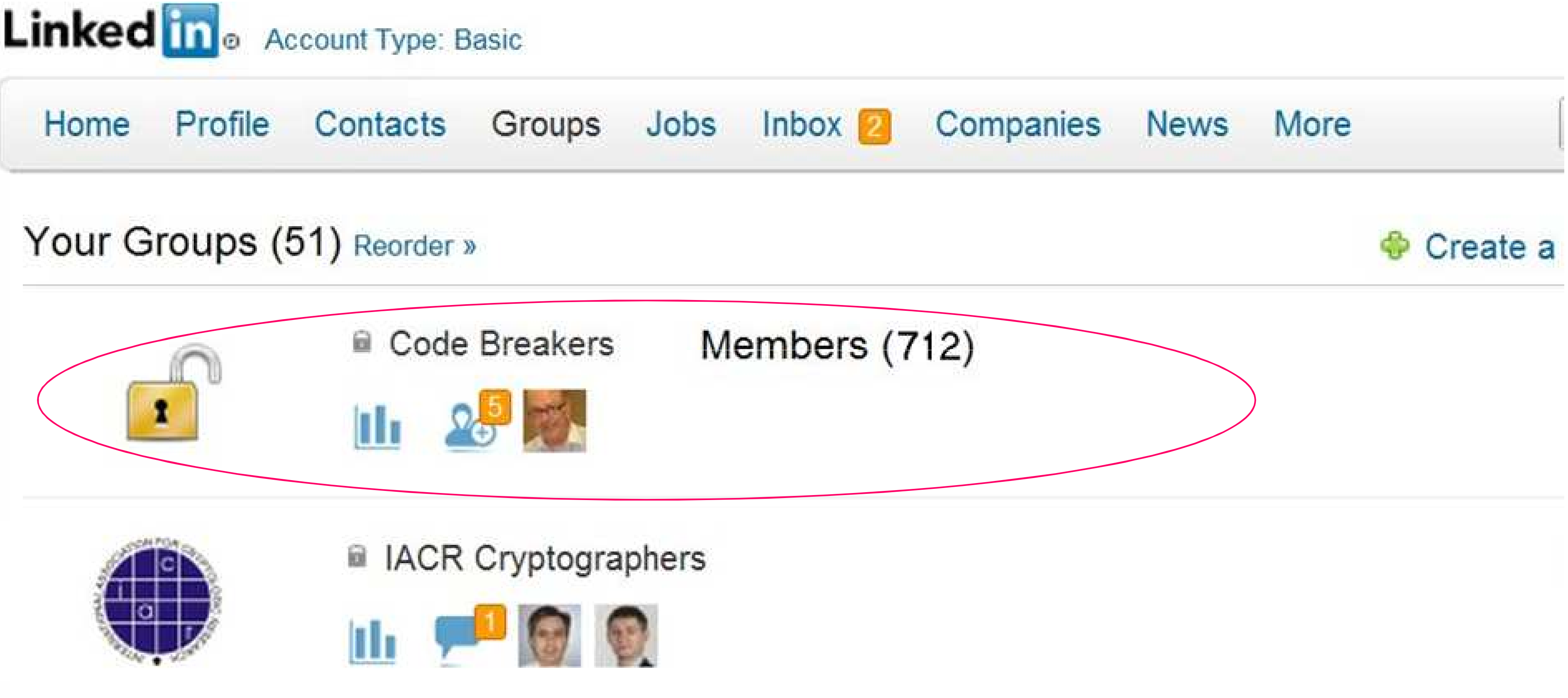
2. payment and smart cards (e.g. bank cards, Oyster cards etc…)

Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

LinkedIn



Linked in Account Type: Basic

Your Groups (51) Reorder »

Create a

Code Breakers Members (712)

IACR Cryptographers

UCL Bitcoin Seminar

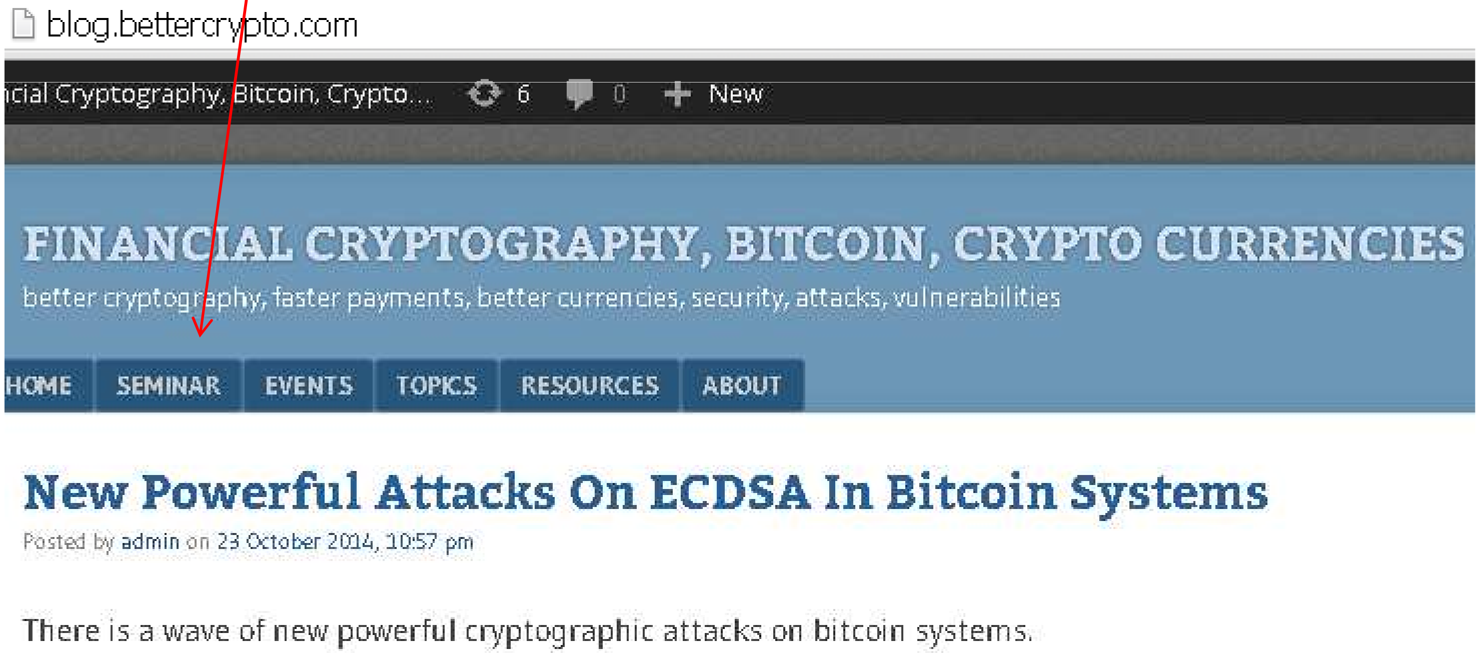
research seminar

=>In central London, runs EVERY WEEK!

public web page:

blog.bettercrypto.com / SEMINAR

or Google "UCL bitcoin seminar"



blog.bettercrypto.com

FINANCIAL CRYPTOGRAPHY, BITCOIN, CRYPTO CURRENCIES

better cryptography, faster payments, better currencies, security, attacks, vulnerabilities

New Powerful Attacks On ECDSA In Bitcoin Systems

Posted by admin on 23 October 2014, 10:57 pm

There is a wave of new powerful cryptographic attacks on bitcoin systems.

My Whole Life:

Tried to improve

the security baseline…

My Whole Life:

Tried to improve
    the security baseline…

Crying Wolf!

51%, Elliptic Curve, OpenSSL...

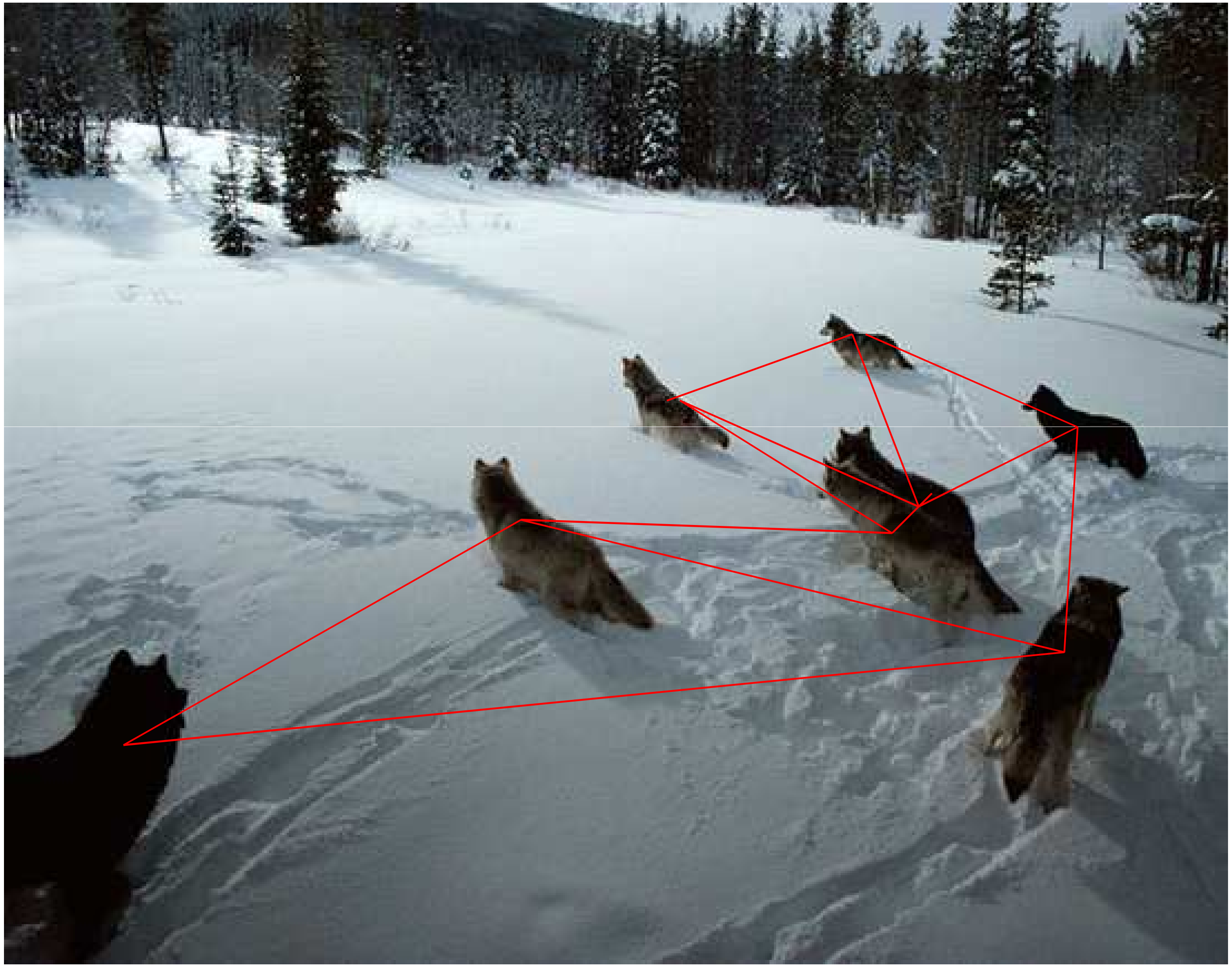
It did NOT help,

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:

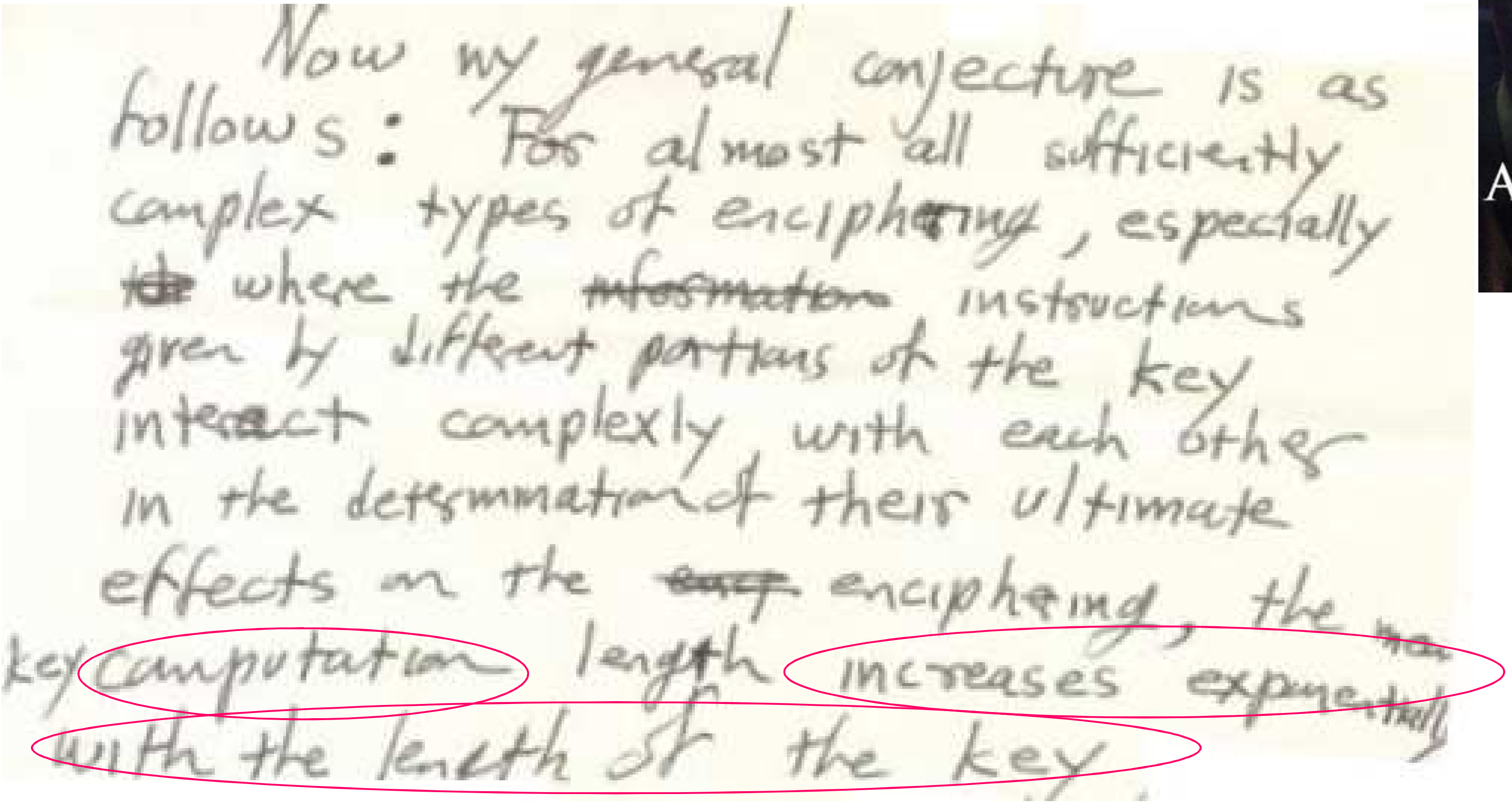
[…] actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs.

[…] Insert vulnerabilities into commercial encryption systems […]

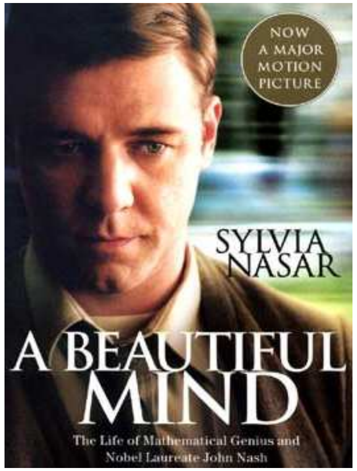
[…] Influence policies, standards and specification for commercial public key technologies.[…]

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

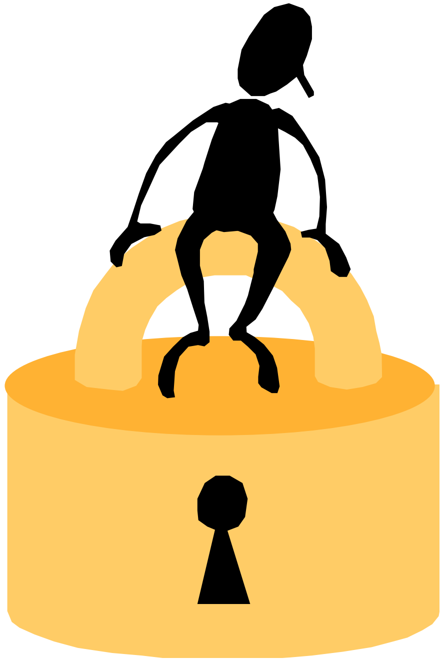

NOW A MAJOR MOTION PICTURE
SYLVIA NASAR
A BEAUTIFUL MIND
The Life of Mathematical Genius and Nobel Laureate John Nash

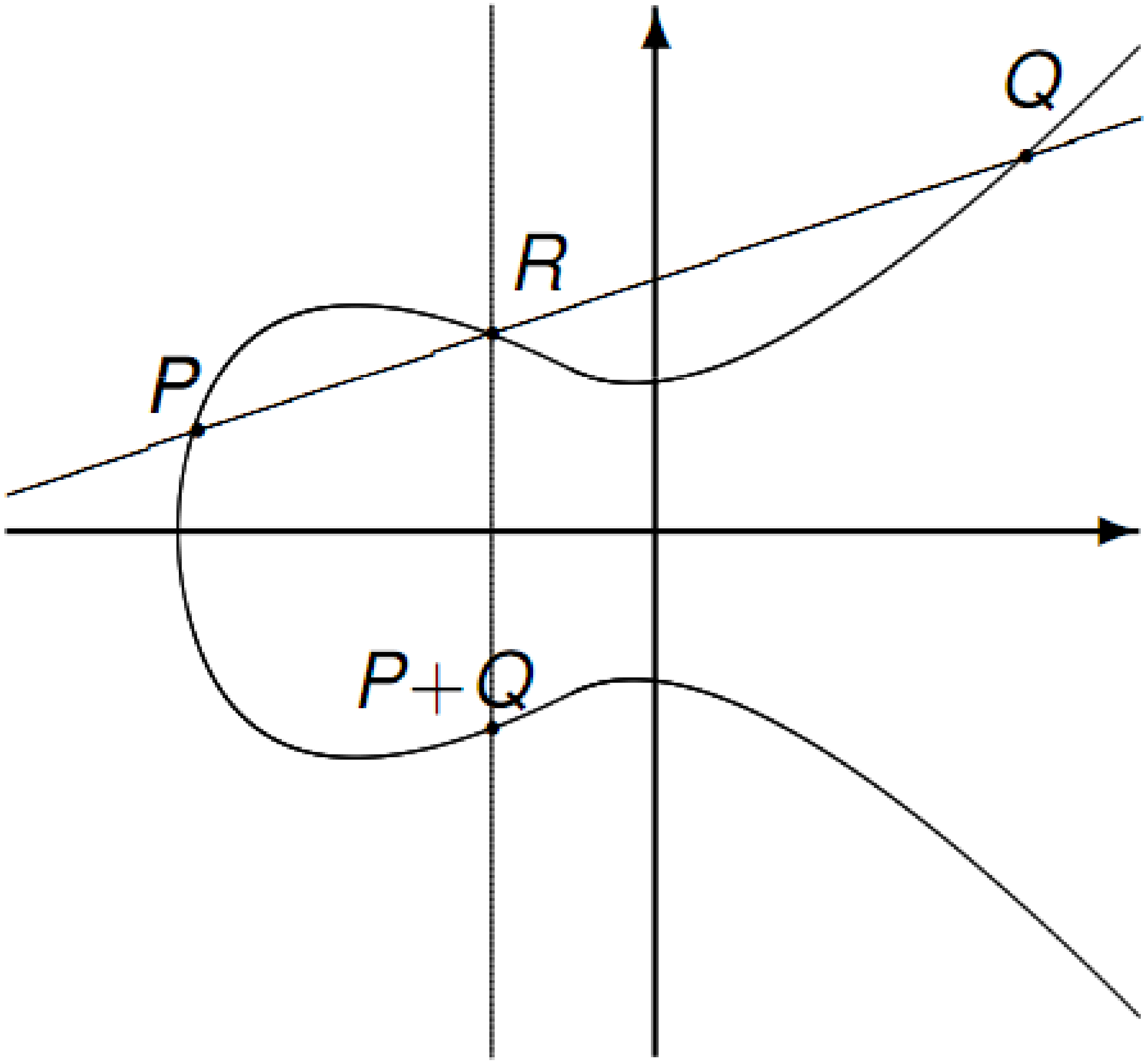
He also says that:

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

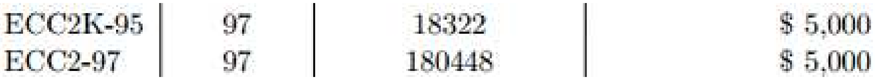
Elliptic Curve Crypto

“exponential security”

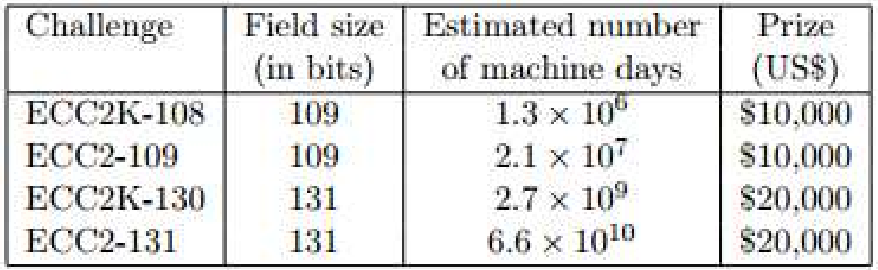




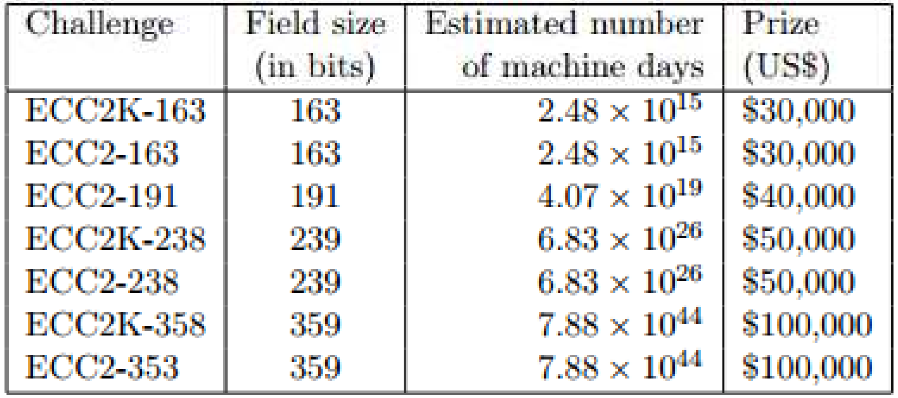
ECC - Certicom Challenges [1997, revised 2009]



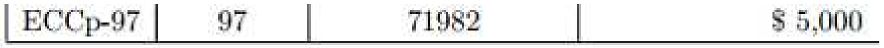
ECC2K-95	97	18322	$ 5,000
ECC2-97	97	180448	$ 5,000



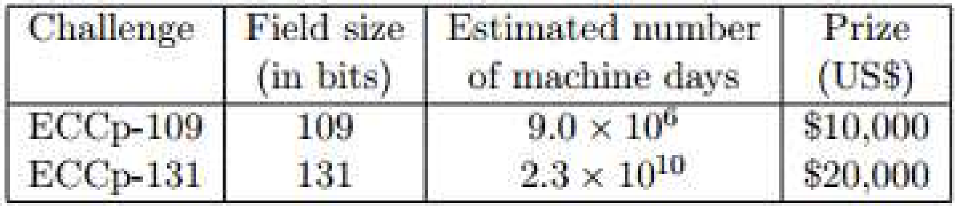
Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECC2K-108	109	1.3×10^6	$10,000
ECC2-109	109	2.1×10^7	$10,000
ECC2K-130	131	2.7×10^9	$20,000
ECC2-131	131	6.6×10^{10}	$20,000



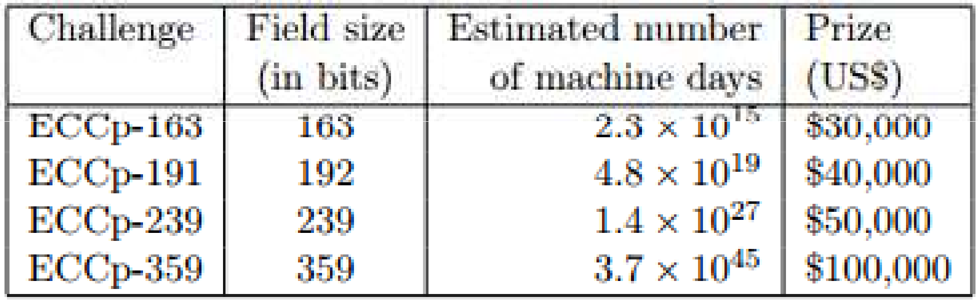
Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECC2K-163	163	2.48×10^{15}	$30,000
ECC2-163	163	2.48×10^{15}	$30,000
ECC2-191	191	4.07×10^{19}	$40,000
ECC2K-238	239	6.83×10^{26}	$50,000
ECC2-238	239	6.83×10^{26}	$50,000
ECC2K-358	359	7.88×10^{44}	$100,000
ECC2-353	359	7.88×10^{44}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

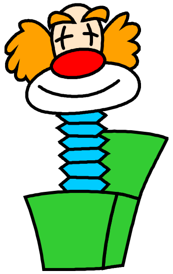
TOTAL = 725,000 USD

P vs. NP

- If you solve P vs. NP it: 1 M$.
- Nobel price, Abel price in mathematics: roughly 1M$
- Break bitcoin ECC: About 4 BILLION $.

How to Steal Bitcoins

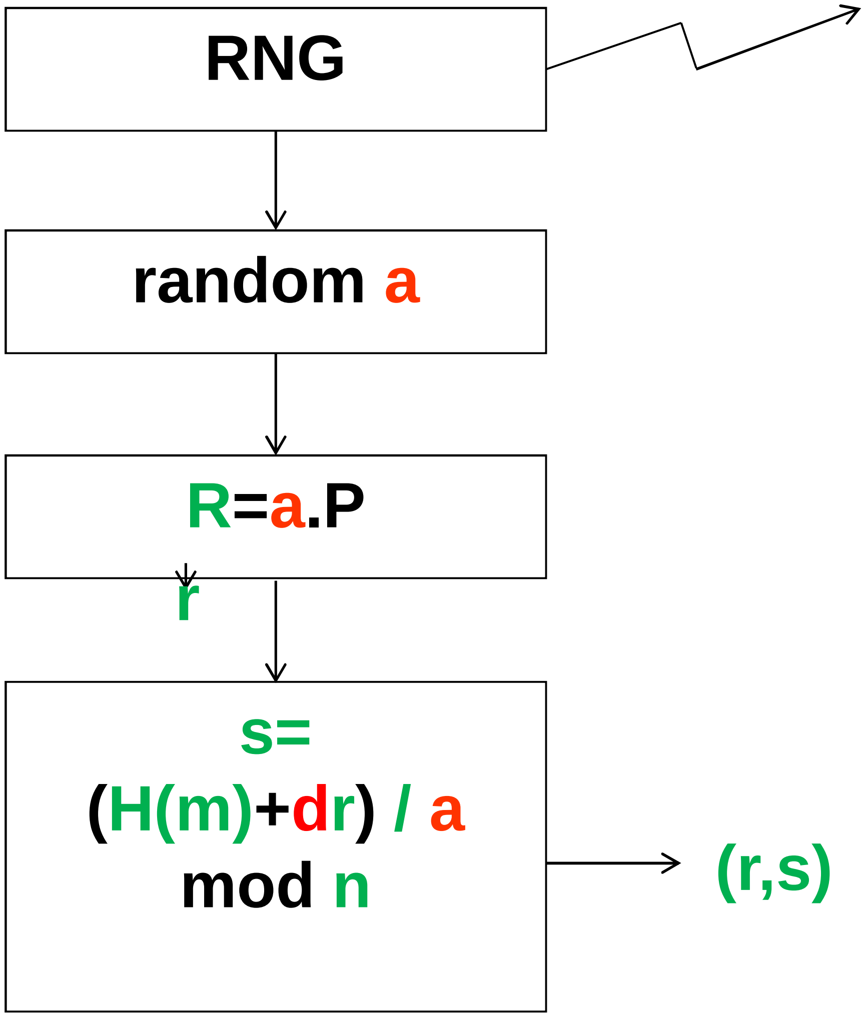
New attacks [Courtois et al. October 2014]



ECDSA Attack – 2 Users

has already happened 100 times in Bitcoin

random a: must be kept secret!



same a used twice => detected in public blockchain =>

$$(s_1 a - H(m_1))/d_1 = r = (s_2 a - H(m_2))/d_2 \bmod n$$

$$\Rightarrow$$

$$r(d_1 - d_2) + a(s_1 - s_2) = H(m_2) - H(m_1) \bmod n$$

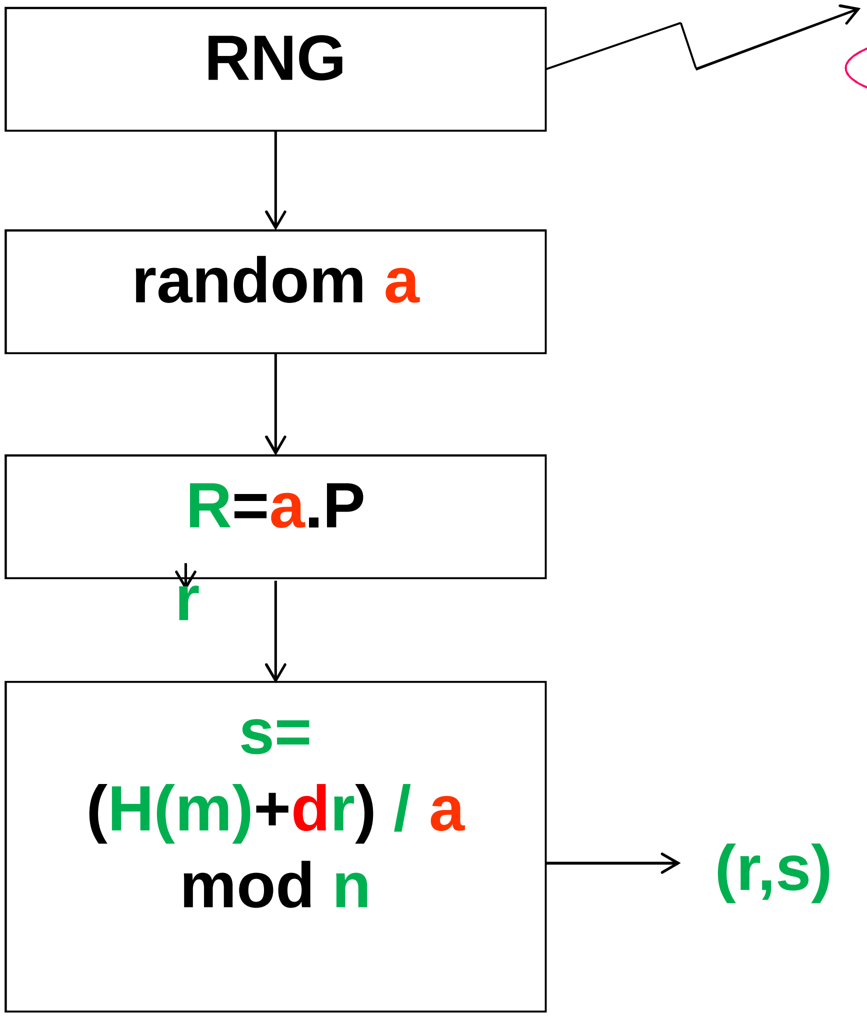
each person can steal the other person's bitcoins!

=>any of them CAN recompute k used

Attack – Same User

has also happened 100 times in Bitcoin

random a: must be kept secret!



RNG

random a

R=a.P

r

s= (H(m)+dr) / a mod n

(r,s)

same a used twice by the same user ($d_1=d_2$). In this case we have: $(s_1 a - H(m_1))$ = rd = $(s_2 a - H(m_2))$ mod n

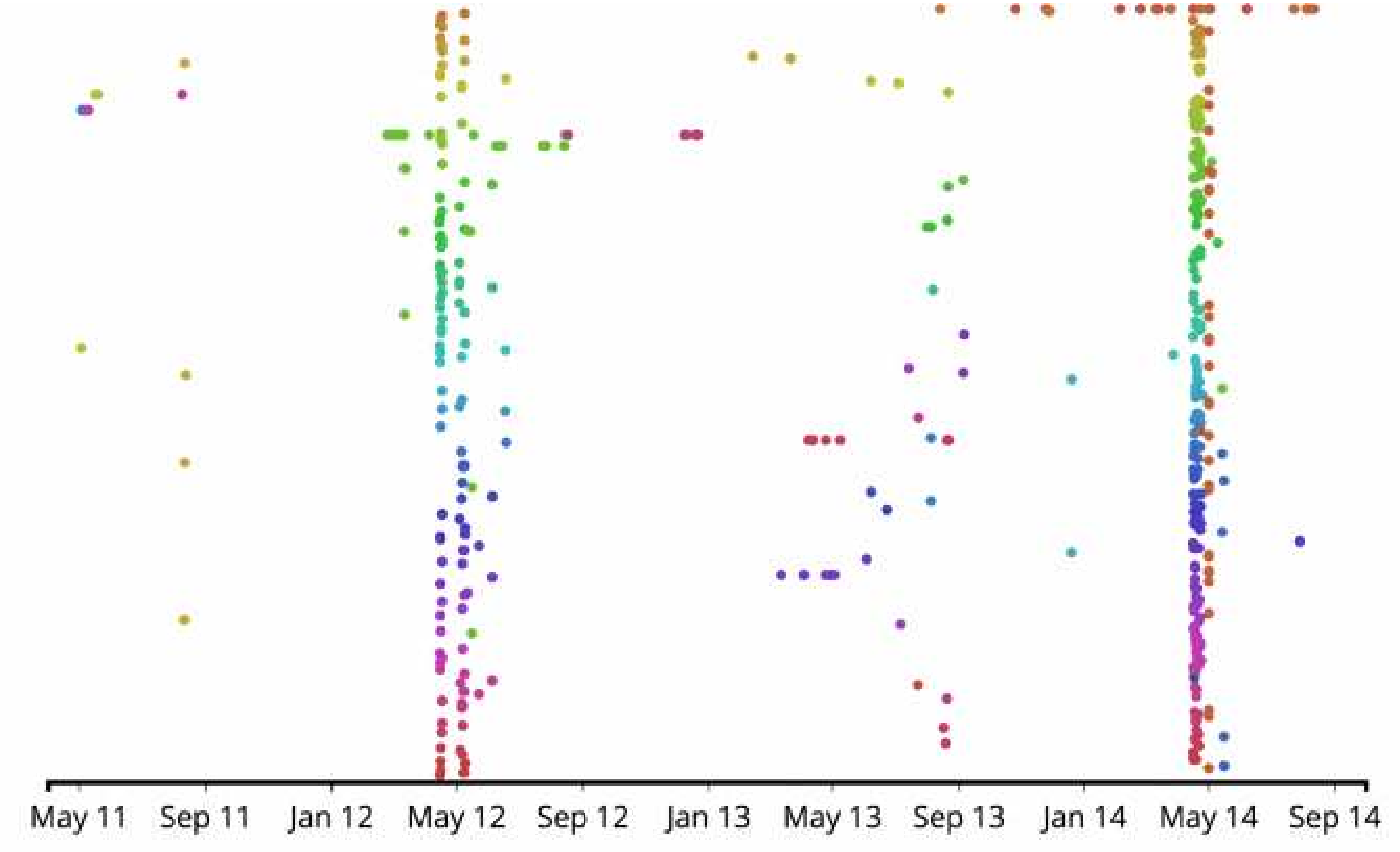
=> $a=(H(m_1)- H(m_2))/(s_1-s_2)$ mod n AND now $d=(sa-H(m))/r$ mod n

anybody can steal the bitcoins!

Stopped in 2013?

Android bug was fixed…

Second Major Outbreak – May 2014



Recent Bad Randoms

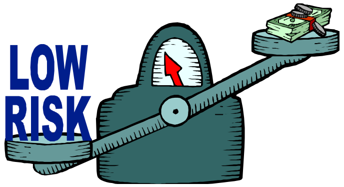
From my own scan:

0f25a7cc9e76ef38c0feadcfa5550c173d845ce36e16bde09829a3af57097240.

Appears 8 times in block 322925

28 September 2014

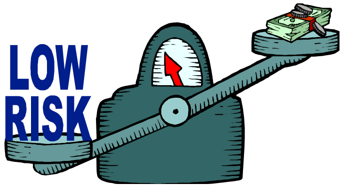
Used by different users…



So What?

Previous attacks:

- Classical bad random attacks typically concern only very few bitcoin accounts, and only some very lucky holders of bitcoins can actually steal other people's bitcoins.
- Only a few hundred accounts in the whole history of bitcoin are affected.



The Really Scary Attacks

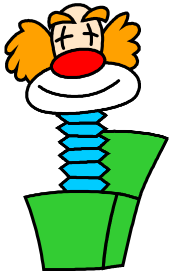
New attacks [Courtois et al. October 2014]

=> under certain conditons

ALL bitcoins in cold storage

can be stolen

=>millions of accounts potentially affected.



New Paper:

Private Key Recovery Combination Attacks:
On Extreme Fragility of Popular Bitcoin Key Management, Wallet and Cold Storage Solutions in Presence of Poor RNG Events

Nicolas T. Courtois[1] Pinar Emirdag[2] Filippo Valsorda[3]

[1] University College London, UK
[2] Independent market structure professional, London, UK
[3] CloudFlare, London, UK

Abstract. In this paper we study the question of key management and practical operational security in bitcoin digital currency storage systems. We study the security two most used bitcoin HD Wallet key management solutions (e.g. in BIP032 and in earlier systems). These systems have extensive audit capabilities but this property comes at a very high price. They are excessively fragile. One small security incident in a remote corner of the system and everything collapses, all private keys can be recovered and ALL bitcoins within the remit of the system can be stolen. Privilege escalation attacks on HD Wallet solutions are not new. In this paper we take it much further. We propose new more advanced **combination attacks** in which the security of keys hold in cold storage can be compromised without executing any software exploit on the cold system, but through security incidents at operation such as **bad random number or related random events**.

In our new attacks all bitcoins over whole large security domains can be stolen by people who have the auditor keys which are typically stored in hot systems connected to the Internet and can be stolen easily. Our combination attacks allow to recover private keys which none of the

cf.

eprint.iacr.org/2014/848/

Solutions:

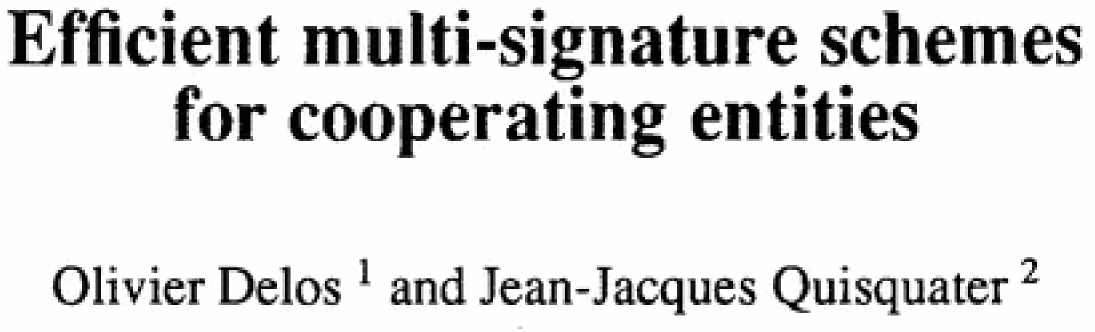
Solution 1: RFC6979 [Thomas Pornin]

Solution 2: MultiSig:

For example 2 out of 3 signatures are required to spend bitcoins.

BTW. Multi-Sig Concept is NOT new…

1993



Efficient multi-signature schemes for cooperating entities

Olivier Delos [1] and Jean-Jacques Quisquater [2]

How to
Un-corrupt Cryptography

Crypto Challenges:

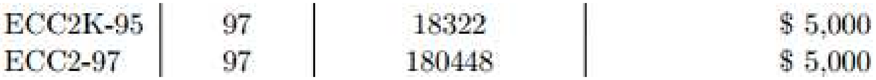
I always liked this idea.

Claiming (very naive) that this would:

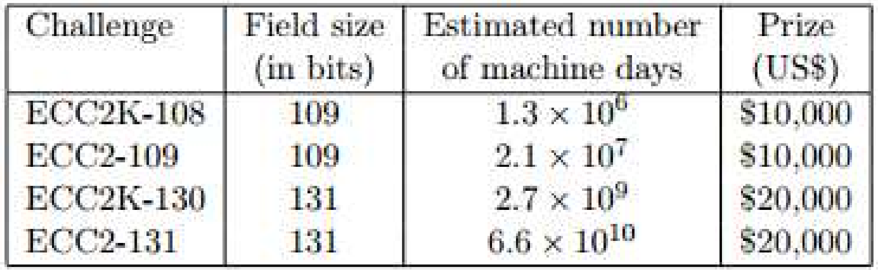
"punish those who
by their ignorance, incompetence
or because of a hidden agenda,
put everybody's security at a great risk."

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

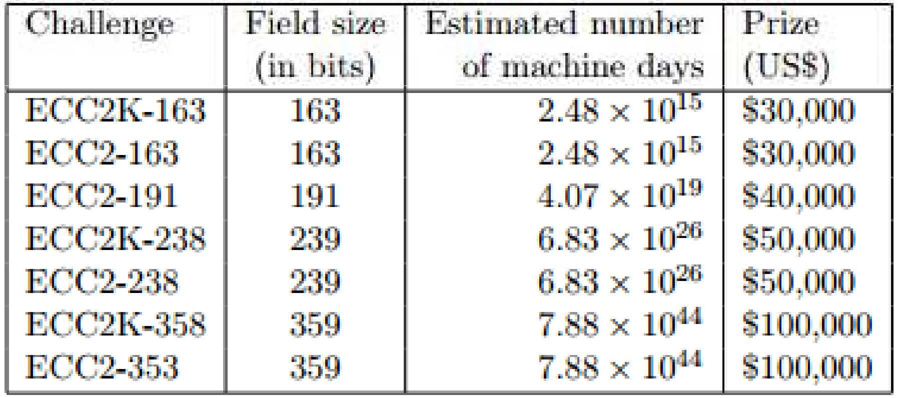
ECC - Certicom Challenges [1997, revised 2009]



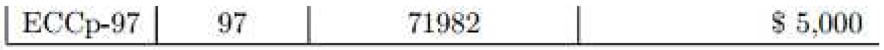
ECC2K-95	97	18322	$ 5,000
ECC2-97	97	180448	$ 5,000



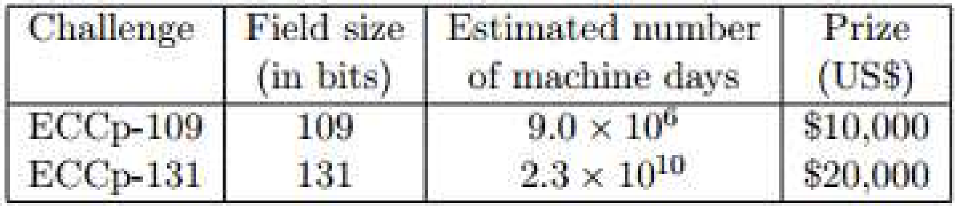
Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECC2K-108	109	1.3×10^6	$10,000
ECC2-109	109	2.1×10^7	$10,000
ECC2K-130	131	2.7×10^9	$20,000
ECC2-131	131	6.6×10^{10}	$20,000



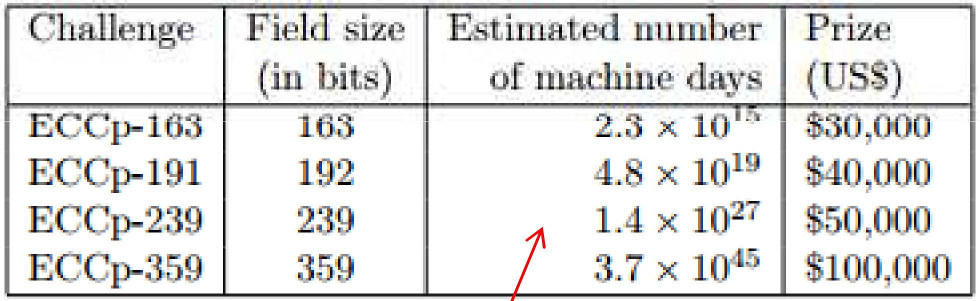
Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECC2K-163	163	2.48×10^{15}	$30,000
ECC2-163	163	2.48×10^{15}	$30,000
ECC2-191	191	4.07×10^{19}	$40,000
ECC2K-238	239	6.83×10^{26}	$50,000
ECC2-238	239	6.83×10^{26}	$50,000
ECC2K-358	359	7.88×10^{44}	$100,000
ECC2-353	359	7.88×10^{44}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

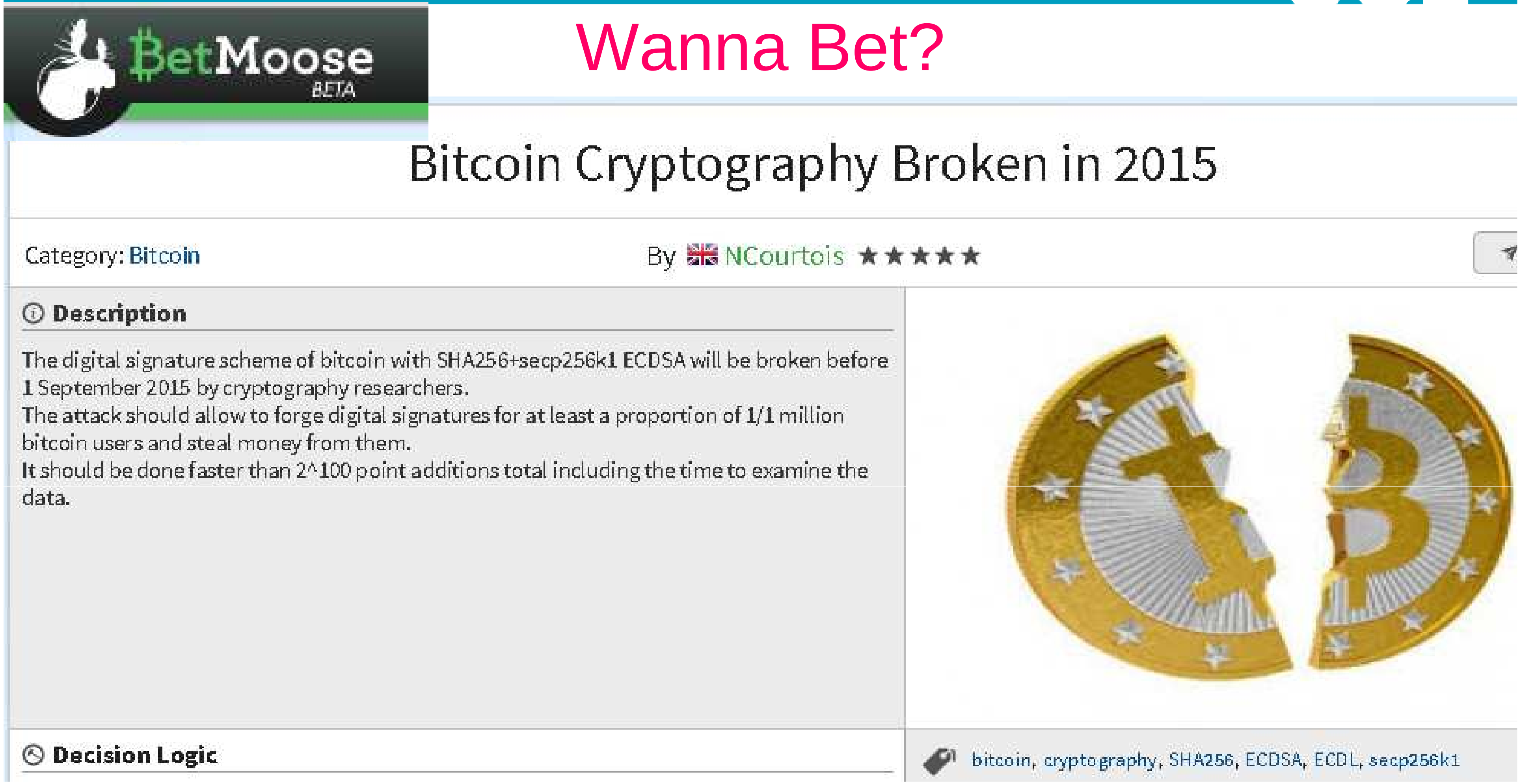
``I did not know that BitCoin is using secp256k1.
I am surprised to see anybody use secp256k1 instead of secp256r1'',

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 ★★★★★

Description

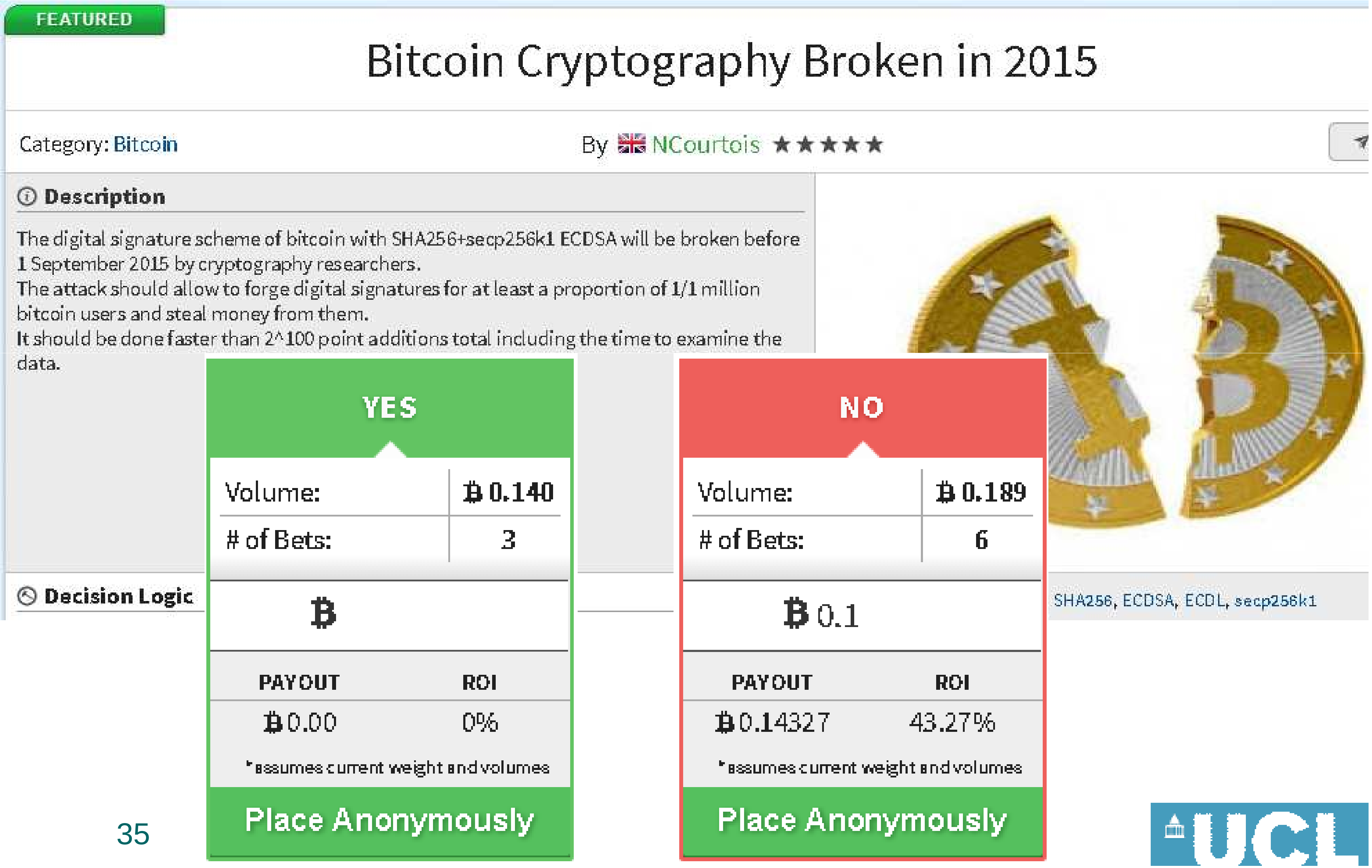
The digital signature scheme of bitcoin with SHA256+secp256k1 ECDSA will be broken before 1 September 2015 by cryptography researchers.
The attack should allow to forge digital signatures for at least a proportion of 1/1 million bitcoin users and steal money from them.
It should be done faster than 2^100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

Decision Logic

SHA256, ECDSA, ECDL, secp256k1

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

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…

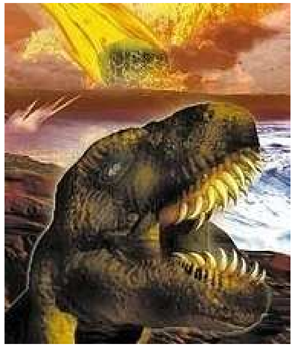
https://www.betmoose.com/bet/bitcoin-cryptography-broken-in-2015-791

- 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!

“Programmed Self-Destruction”

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

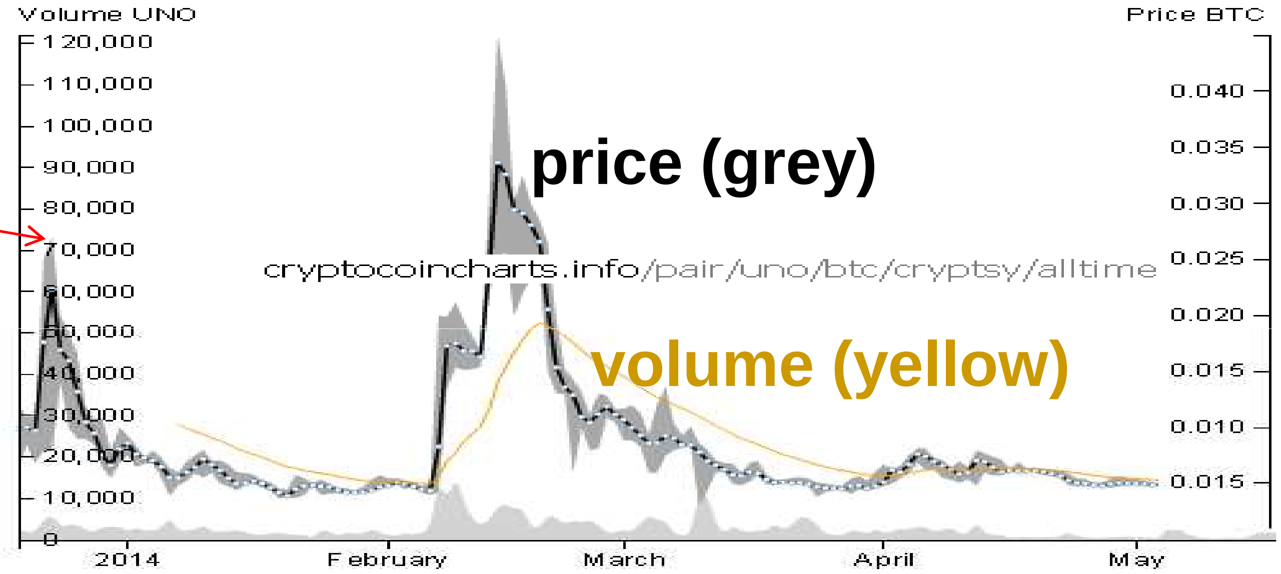


Unobtanium

– pump and dump: evidence

Cause:

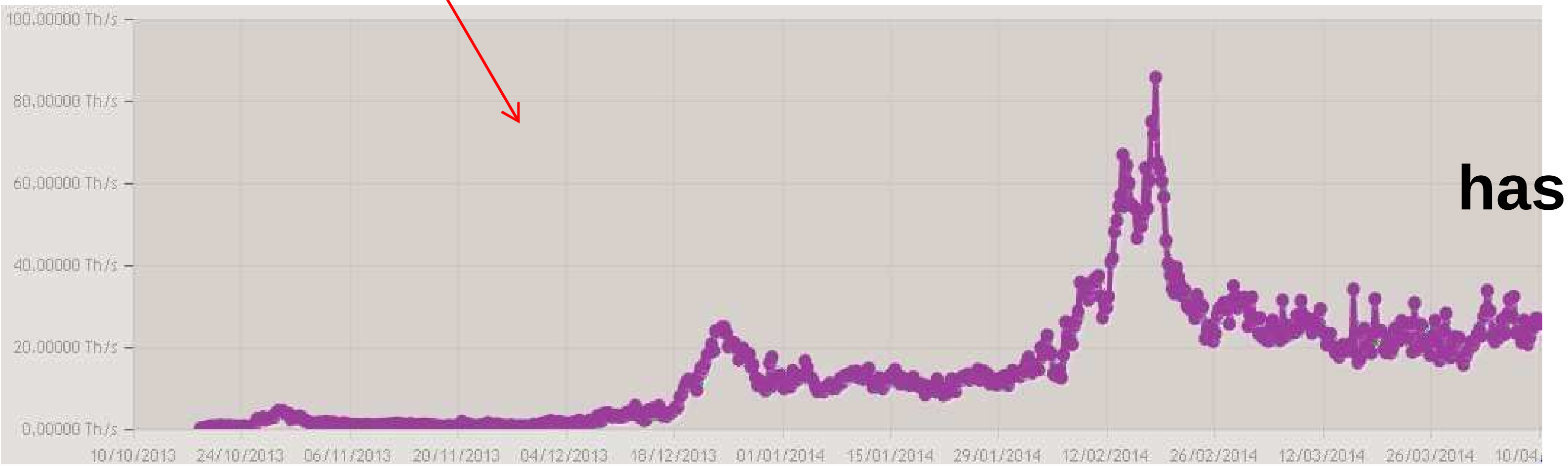
Effect:



price (grey)

cryptocoincharts.info/pair/uno/btc/cryptsy/alltime

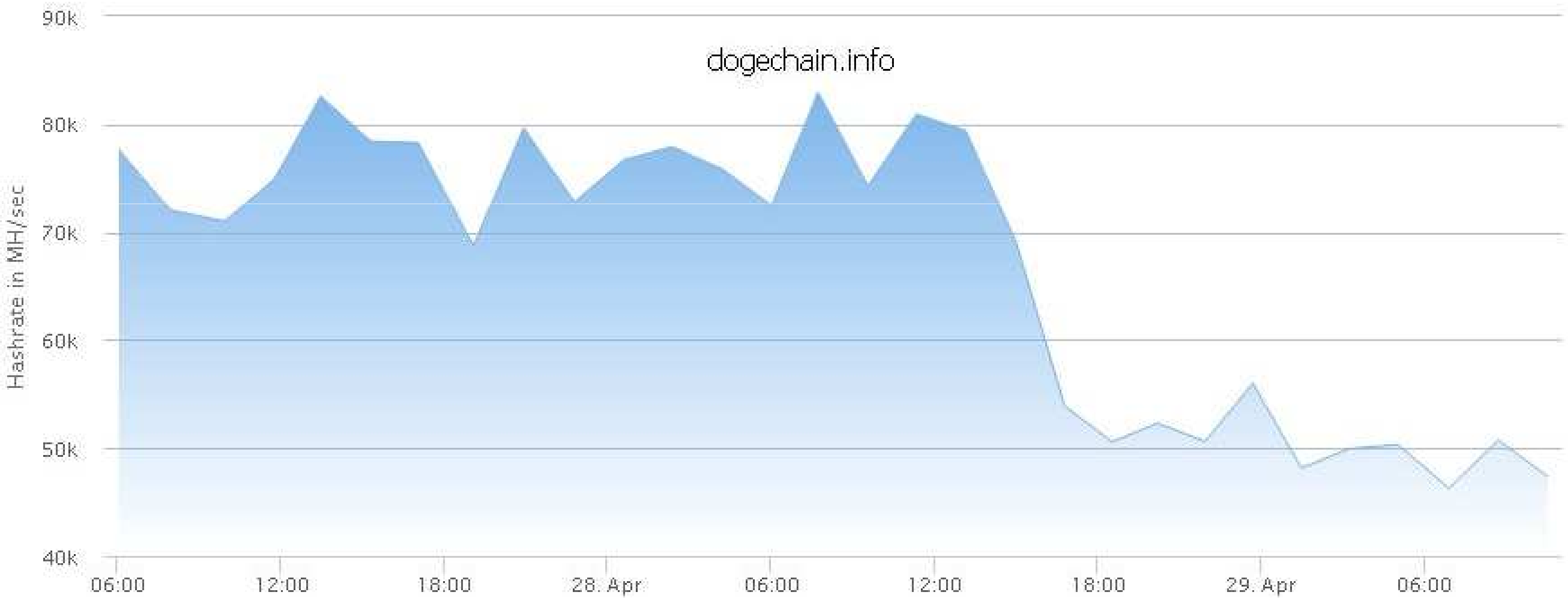
volume (yellow)



hash rate

DogeCoin Predicted Decline [Courtois]

– hash rate MUST decline, as a result of monetary policy



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.

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 [...])"

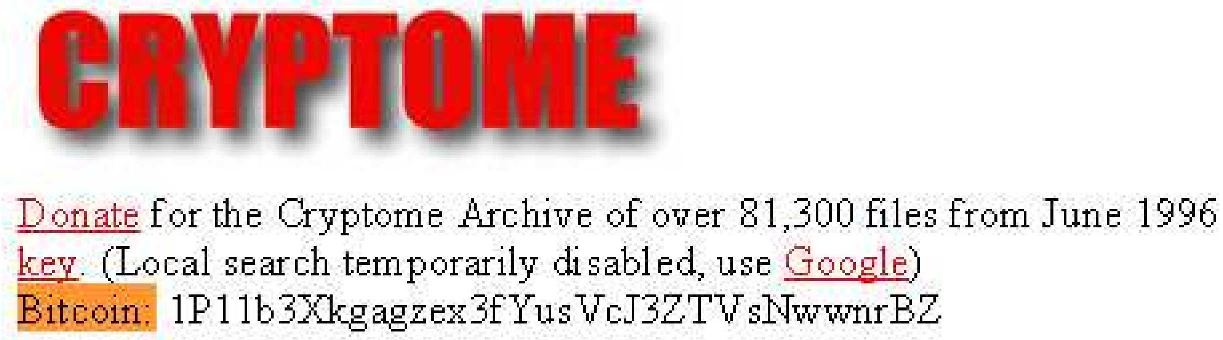
Josh Mohland, 4 August 2014

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 [...])”

=> after the reform Dogecoin Market price more than tripled…

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.

Bitcoin vs.

Security Engineering

Re-Engineering Bitcoin:

We postulate:

[Saltzer and Shroeder 1975]

1. Open design.

2. Least Common Mechanism

3. Assume that attacker controls the Internet [Dolev-Yao model, 1983].

4. The specification should be engineered in such a way that it is hard for developers to make it insecure on purpose (e.g. embed backdoors in the system).

Least Common Mechanism

Violated in Bitcoin:

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

2 July 2014.

At minute 02.55: Dr. Nicolas Courtois of UCL:

“…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."

Least Common Mechanism

Violated in Bitcoin also because it uses:

- Open SSL and other standard libraries with massive amounts of code which is not useful at all for bitcoin
- when using TOR
- etc..

Open Design Principle

[Saltzer and Schroeder 1975]

Open Design ≠ Open Source

Examples: cryptography such as SHA256 (used in bitcoin) is open source but NOT open design – it was designed behind closed doors!

NATIONAL SECURITY AGENCY

Open Source vs. Closed Source and Security

Secrecy:

Very frequently an obvious business decision.

- Creates entry barriers for competitors.
- But also defends against hackers.

Kerckhoffs’ principle: [1883]

“The system must remain secure should it fall in enemy hands …”

Kerckhoffs’ principle: [1883]

Most of the time: incorrectly understood.
Utopia.

No obligation to disclose.

- Security when disclosed.
- Better security when not disclosed.

Yes (1,2,3,4):

1. Military:
   layer the defences.

Yes (2):

2)

Basic economics:

these 3 extra months

(and not more ☹)

are simply worth a

a lot of money.

Yes (3):

3)

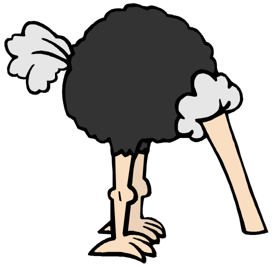
Prevent the erosion of profitability / barriers for entry for competitors / “inimitability”

Yes (4):

4)

Avoid Legal Risks

- companies they don't know where their code is coming from, they want to release the code and they can't because it's too risky!
- re-use of code can COMPROMISE own IP rights and create unknown ROYALTY obligations (!!!)
- clone/stolen code is more stable, more reliable, easier to understand!



What's Wrong
with Open Source?

Kerckhoffs principle:

- Rather WRONG in the world of smart cards…
  - Reasons:
    - side channel attacks,
    - PayTV card sharing attacks
- But could be right elsewhere for many reasons…
  - Example:
    - DES,AES cipher, open-source, never really broken
    - KeeLoq cipher, closed source, broken in minutes…

*Kerckhoffs principle vs. Public Key Crypto vs. Financial Cryptography

- In Public Key Cryptography one key CAN be made public. In practice this means that
  - some group of people has it
  - NO obligation to disclose, to make it really public (and it is almost never done in serious financial applications)
- Again full disclosure for public keys is unbelievably stupid and simply BAD security engineering and BAD security management. Examples:
  - ATMs have like 6 top-level public keys, not really public though
  - in Bitcoin: the public key can remain a secret for years, only a hash is revealed, this is BRILLIANT key management which makes Bitcoin MUCH more secure that it would otherwise be!