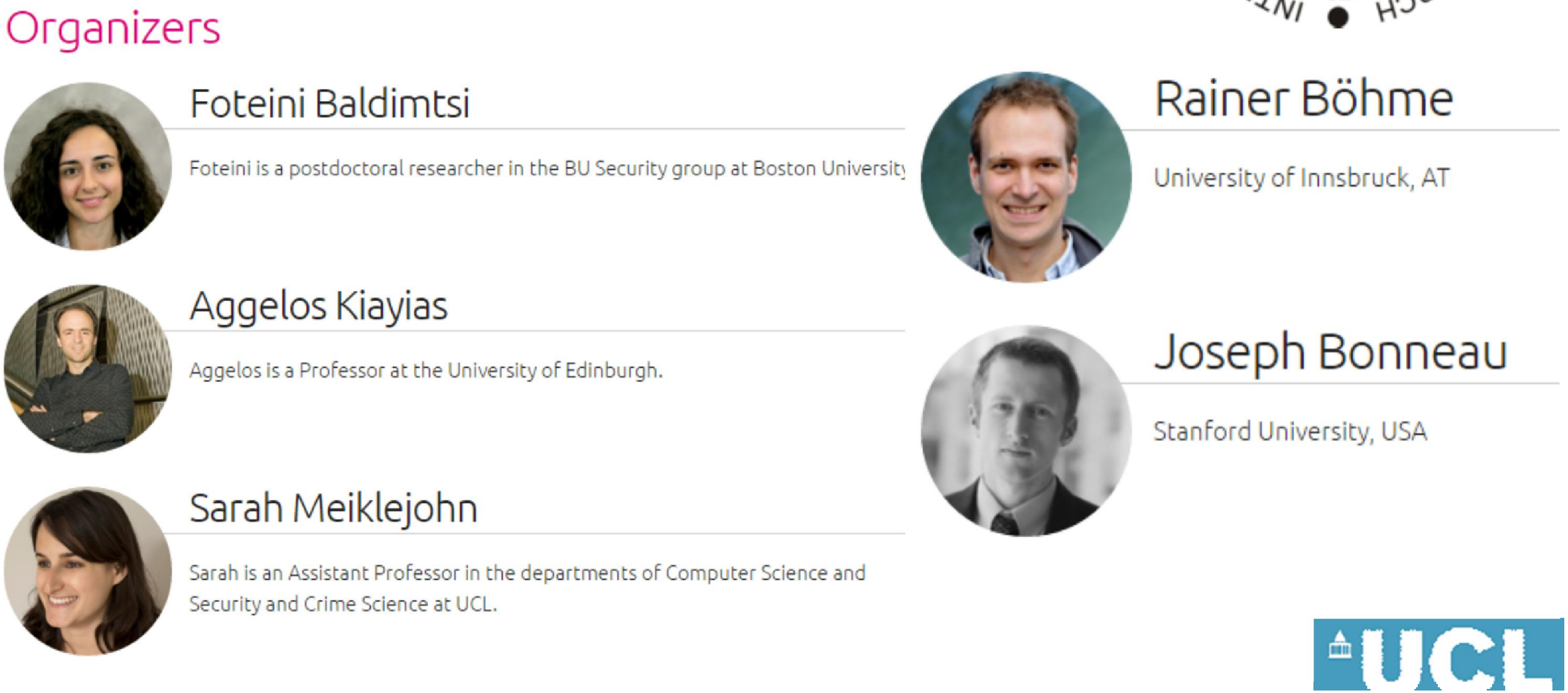
Open Problems in Security of Blockchains

Nicolas T. Courtois

- University College London, UK

Publicité - bitcoinschool.gr

30 May-2 June, Corfu, Greece



Organizers

Foteini Baldimtsi

Foteini is a postdoctoral researcher in the BU Security group at Boston Universit

Aggelos Kiayias

Aggelos is a Professor at the University of Edinburgh.

Sarah Meiklejohn

Sarah is an Assistant Professor in the departments of Computer Science and Security and Crime Science at UCL.

Rainer Böhme

University of Innsbruck, AT

Joseph Bonneau

Stanford University, USA

Roadmap

- How to un-corrupt the planet earth.
- Decentralized self-funded communities
- Bitcoin cryptography and security questions.
- Student research prize fund.

NEW!

Planet Earth A.D. 2016

Dystopian Bastardry and Mafia Economy
Manufacture of Toxic Waste by Debt Slaves

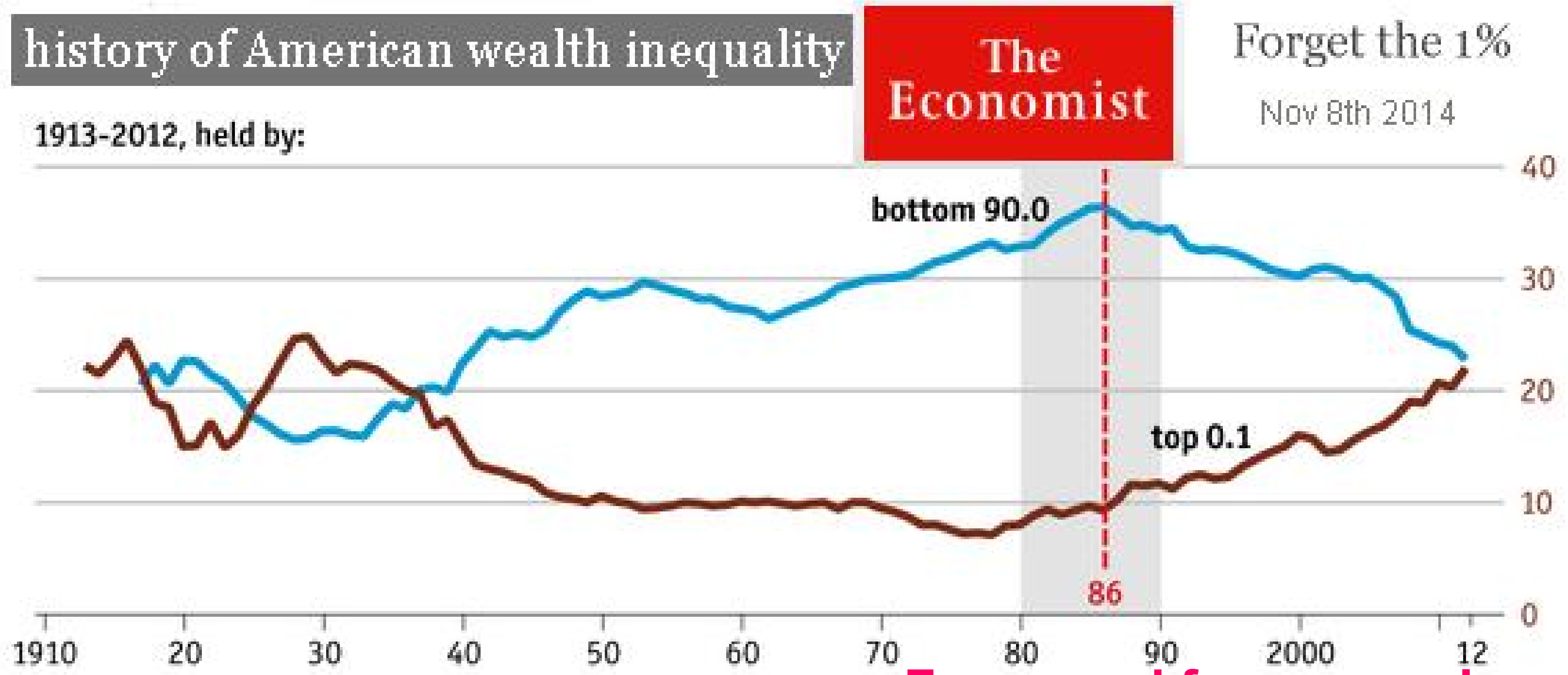
Planet Earth A.D. 2016

Inadequate Responses
Totalitarian + Ignorant

Dystopian Bastardry and Mafia Economy
Manufacture of Toxic Waste by Debt Slaves

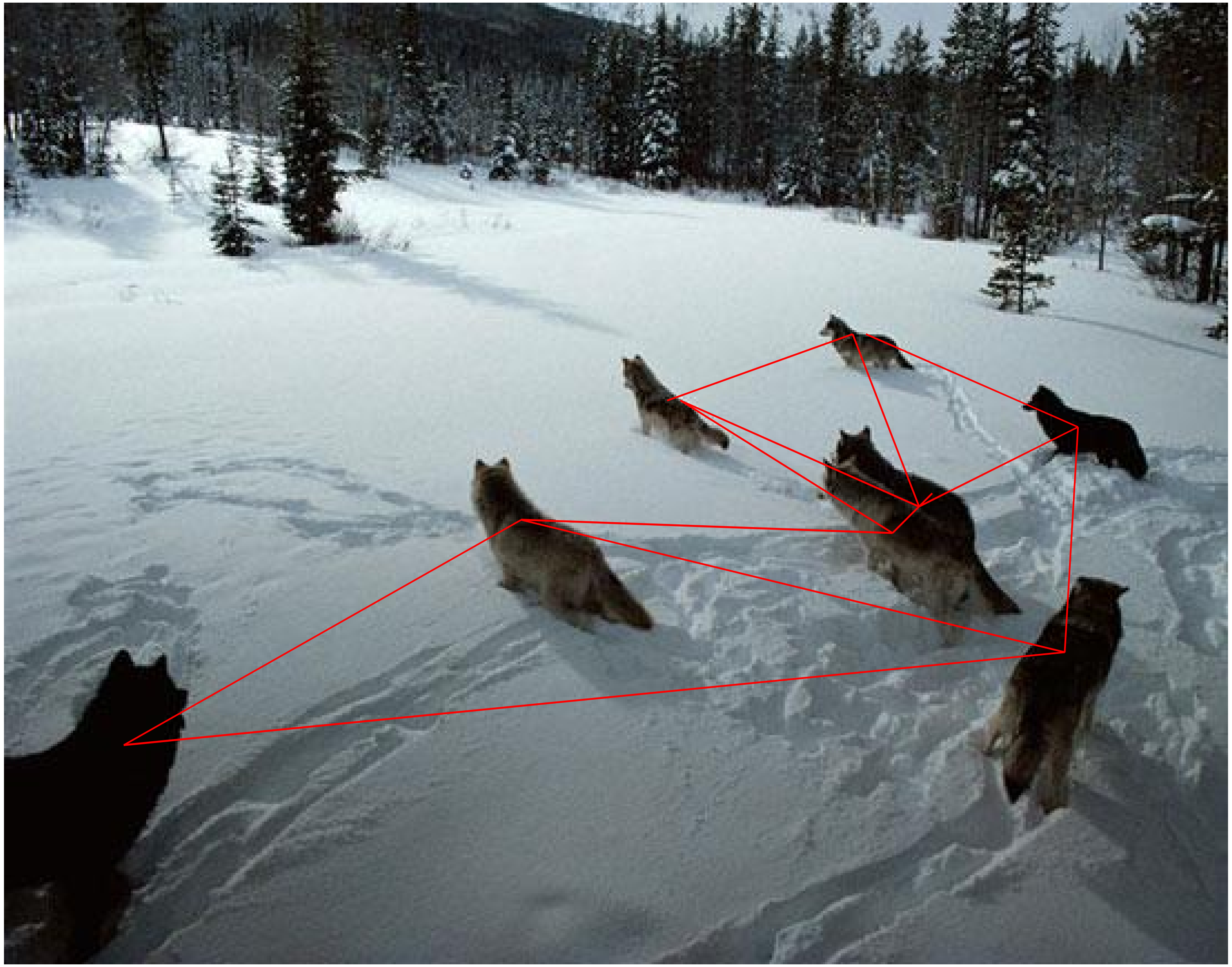
Ordered by the Corrupt Few

Centralization of Power/Money is Real!



Fewer and fewer people…

Solution = Decentralization



New World Order?

There is a growing mood that
nobody can be trusted with our money or our data.

The Telegraph

“the very same people [‘hackers’ or ‘coders’] who helped create these mega-corporations are now working on ‘disruptive technologies’ to replace them.”

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

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.[…]

We failed to protect our DATA

We failed to protect our MONEY

WE'RE BACK!
GOLDMAN SACHS
TAX-PAYER

Miracle Of Bitcoin

Removes two pillars of money:

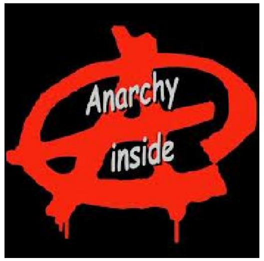
- “trust”

  => P2P self-regulation

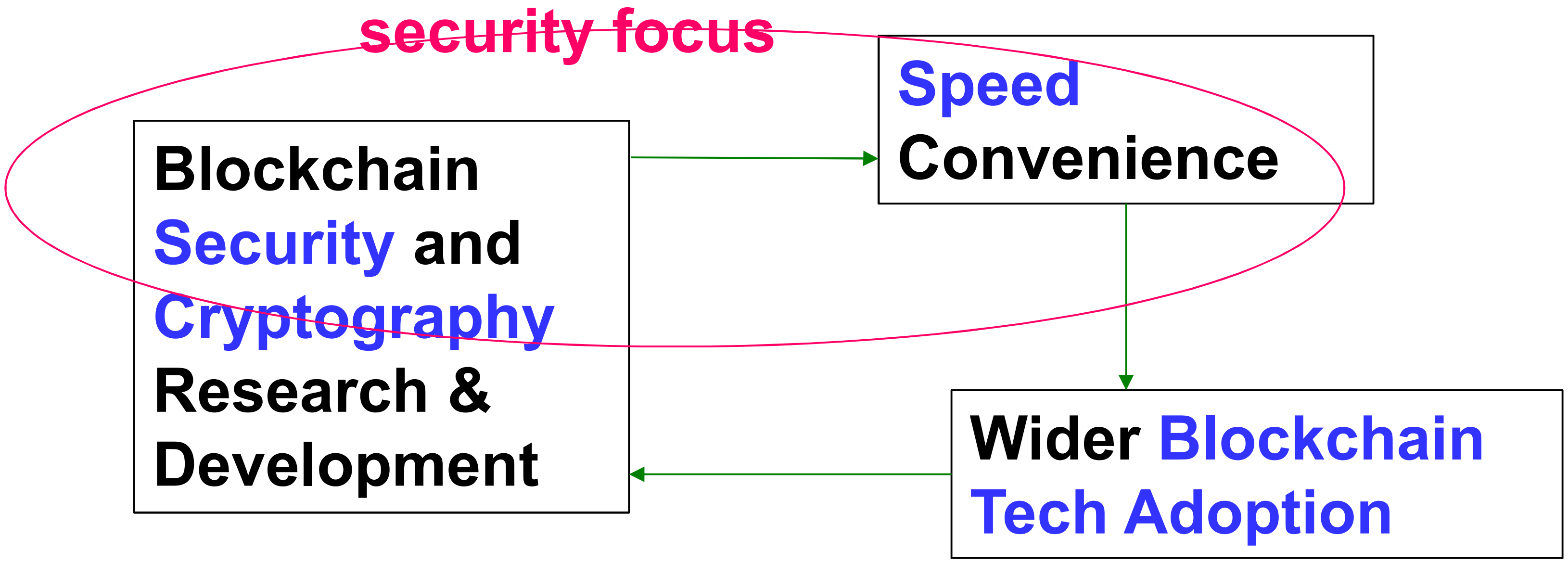
  based on self-interest?

- legal/government protection and policing

  => anarchy!



Virtuous Circle?


security focus
Blockchain Security and Cryptography Research & Development
Speed Convenience
Wider Blockchain Tech Adoption

crypto: enabler technology

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'[...] "

Need For Speed – Open Problems

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

=> Lightning network!

I Also Always Thought That..

$$\text{Speed} \rightarrow \infty$$

$$\Rightarrow$$

$$\text{Security} \rightarrow 0$$

We Can Have (At Least Sometimes)

Speed → ∞

Security → ∞

Security => Speed?

Amazing, normally security and speed are opposites.

In financial markets one can execute trades microseconds.

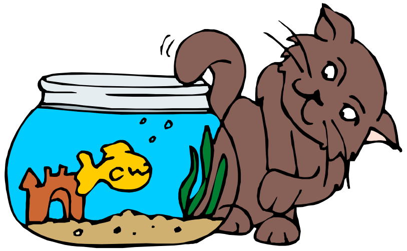
In bitcoin we need to wait for 10 minutes and a large multiple of it for larger transactions.

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.

So Fix the Security Problems!



Questions:

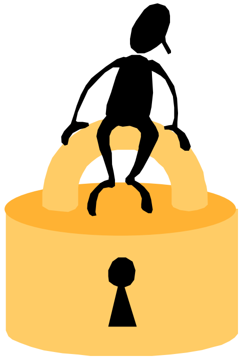
- How can a community of individuals can run a financial cooperative without being manipulated by powerful entities?
- Can we trust the source code and cryptography?

“Cryptographer’s Dream”

- Building “trust-less” systems and a “trust-less” society.

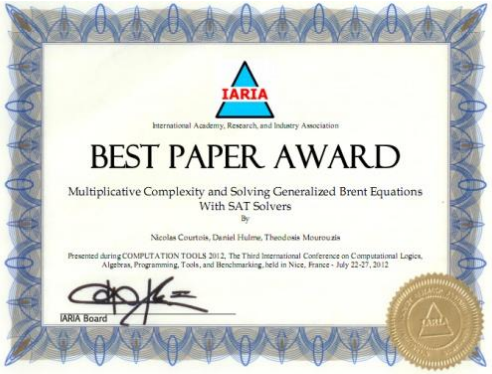
Trust No One?

We still need to
trust the cryptography
(and cryptographers)



Dr. Nicolas T. Courtois

1. cryptologist and codebreaker



IARIA

International Academy, Research, and Industry Association

BEST PAPER AWARD

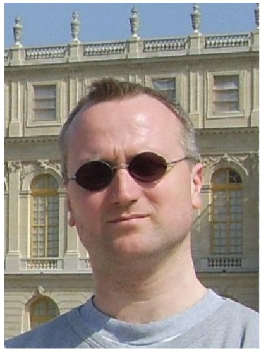
Multiplicative Complexity and Solving Generalized Brent Equations With SAT Solvers

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

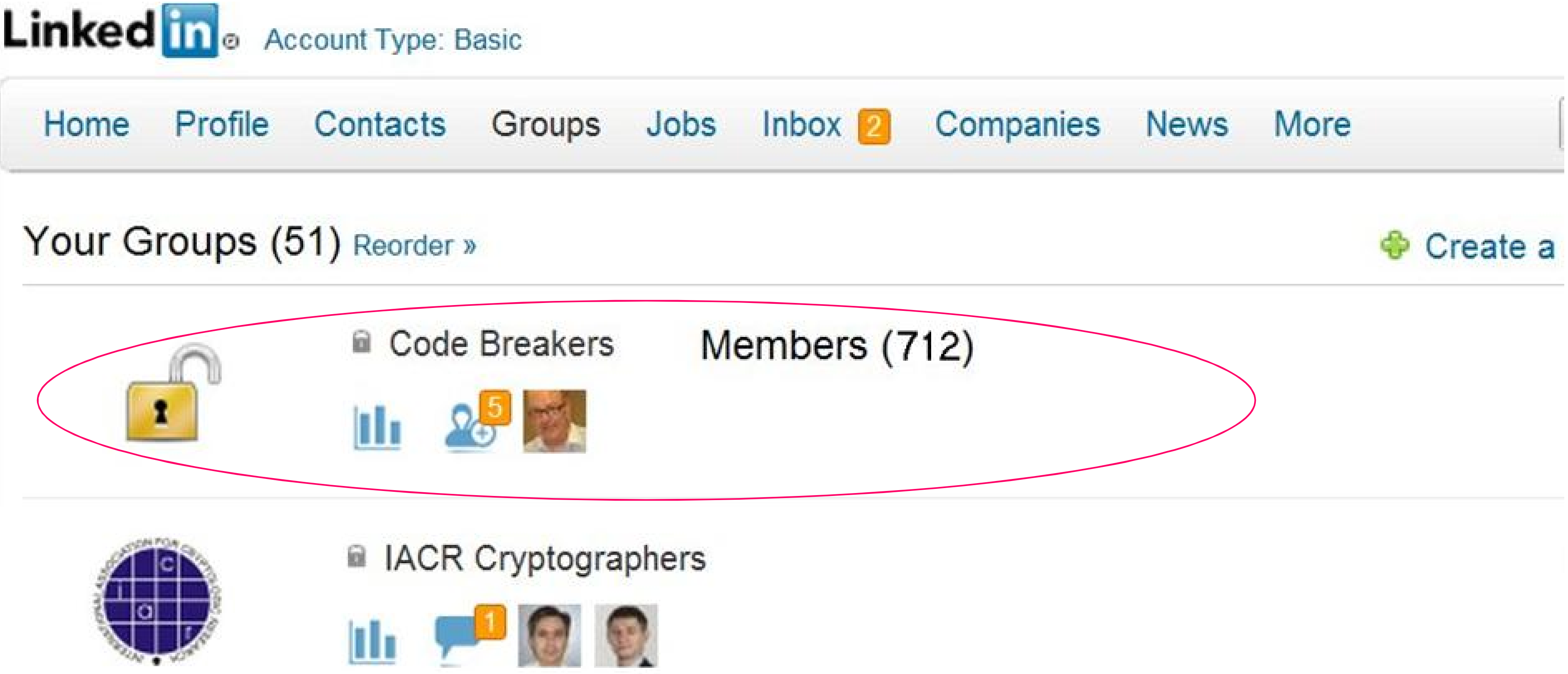
2. payment and smart cards (e.g. bank cards, Oyster cards etc…)

Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

LinkedIn



Account Type: Basic

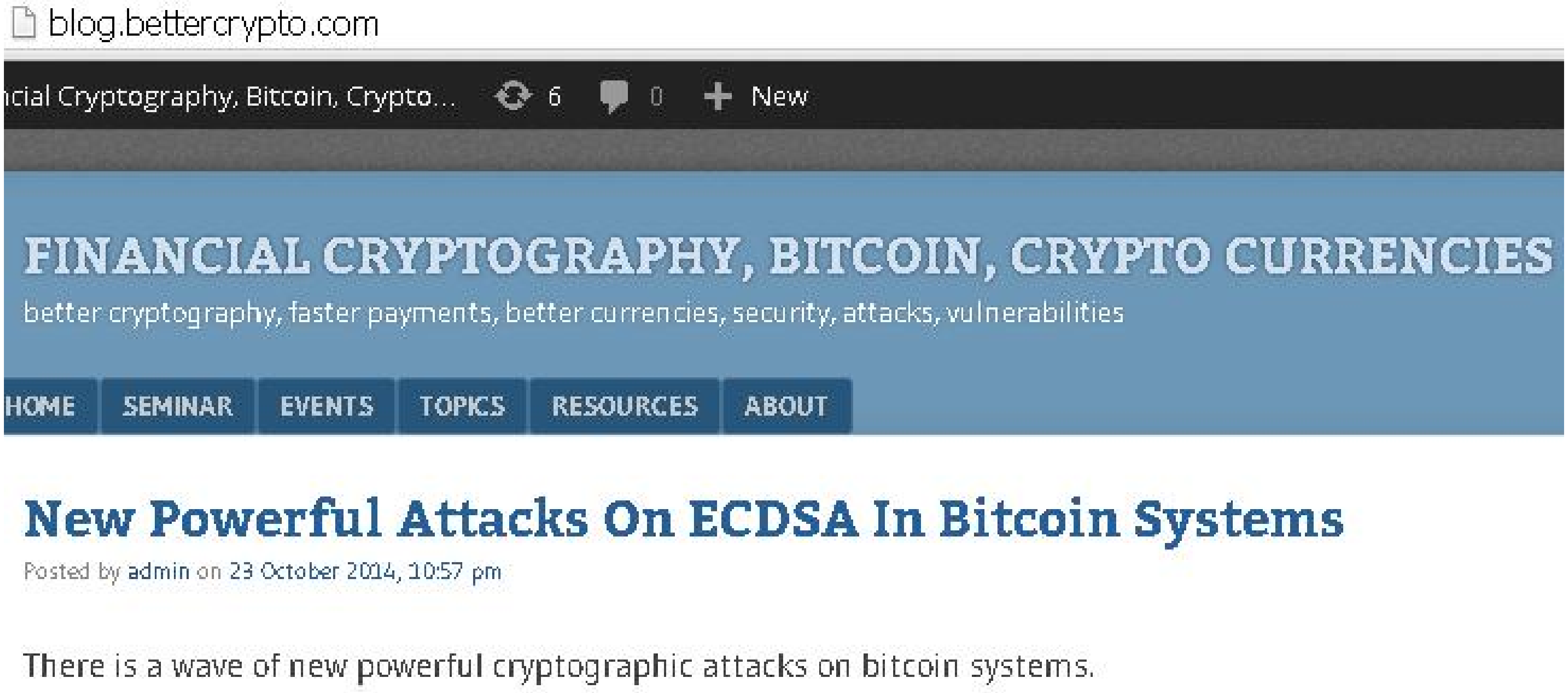
Your Groups (51) Reorder »

Code Breakers Members (712)

IACR Cryptographers

My Blog

blog.bettercrypto.com



blog.bettercrypto.com

FINANCIAL CRYPTOGRAPHY, BITCOIN, CRYPTO CURRENCIES

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

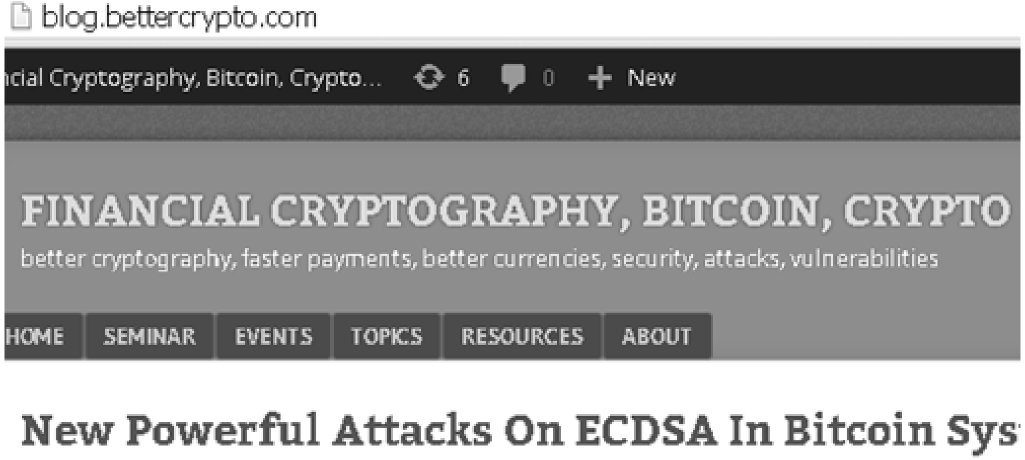
New Powerful Attacks On ECDSA In Bitcoin Systems

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

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

20th Century

- anyone could have a blog…



blog.bettercrypto.com

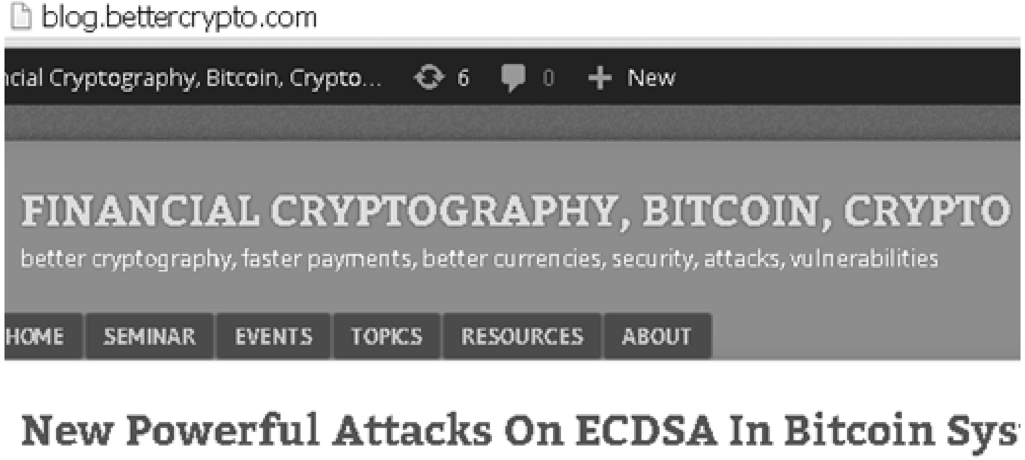
FINANCIAL CRYPTOGRAPHY, BITCOIN, CRYPTO

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

New Powerful Attacks On ECDSA In Bitcoin Sys

21st Century:

- anyone could have a blog…


blog.bettercrypto.com

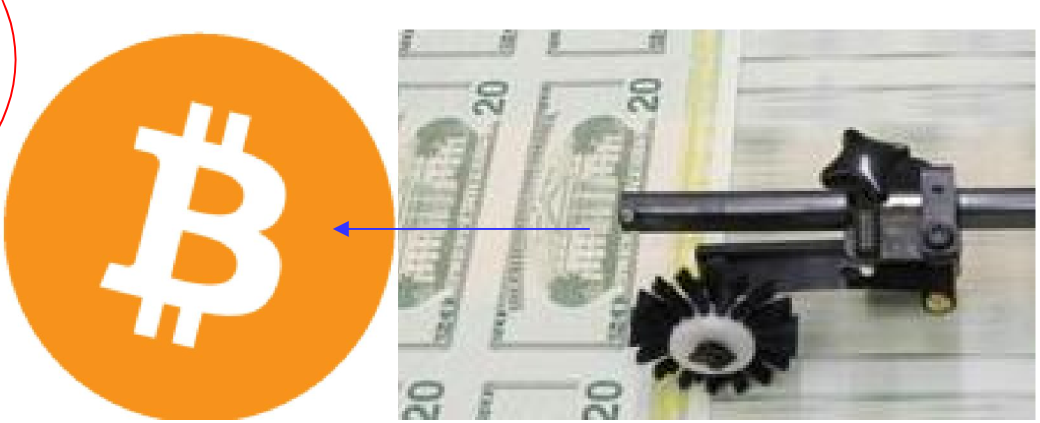
ncial Cryptography, Bitcoin, Crypto…

FINANCIAL CRYPTOGRAPHY, BITCOIN, CRYPTO

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

New Powerful Attacks On ECDSA In Bitcoin Sys

- anyone can print his own currency!



Bitcoin

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 TOTTALLY 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

Citation

Bitcoin is:

- Wild West of our time [Anderson-Rosenberg]

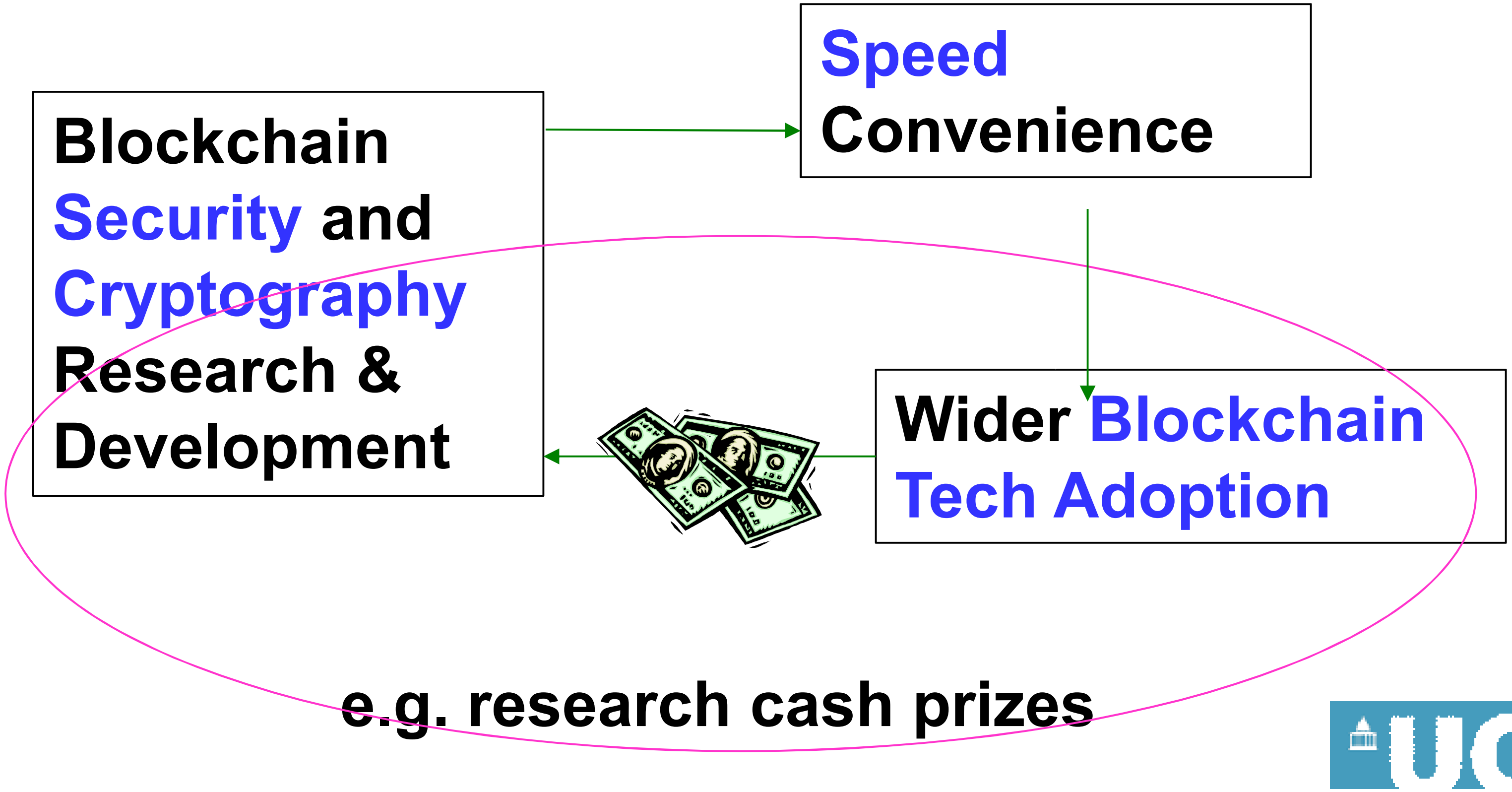
Dangers of Open Source

- 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.

Self-Funding Connection



Blockchain Security and Cryptography Research & Development

Speed Convenience

Wider Blockchain Tech Adoption

e.g. research cash prizes

Improve Quality/Security?

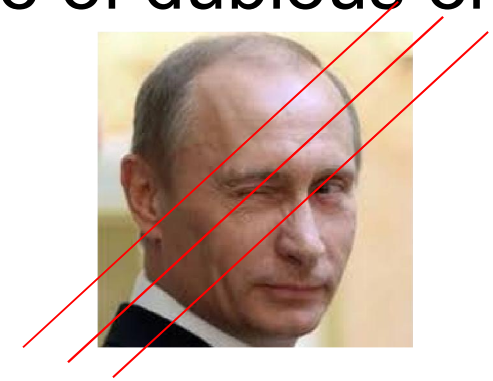
Bitcoin Has The Solution!

Future belongs to

self-funded open-source communities

⇒ can hire programmers, security experts, etc…

⇒ avoid code of dubious origin



Crypto Challenges:

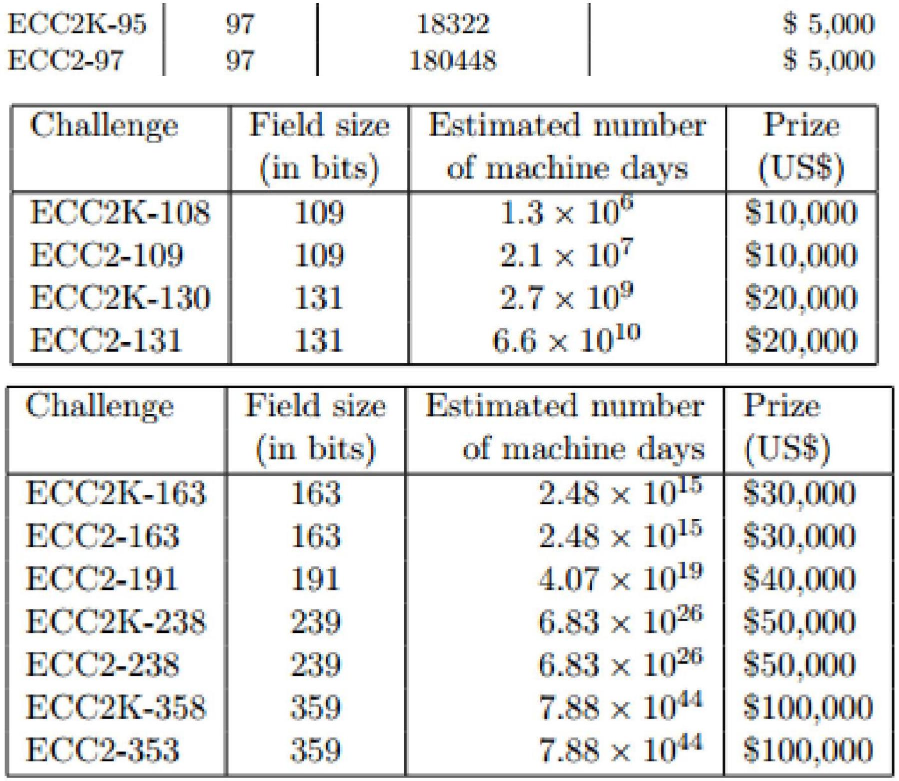
I always liked this idea.

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]

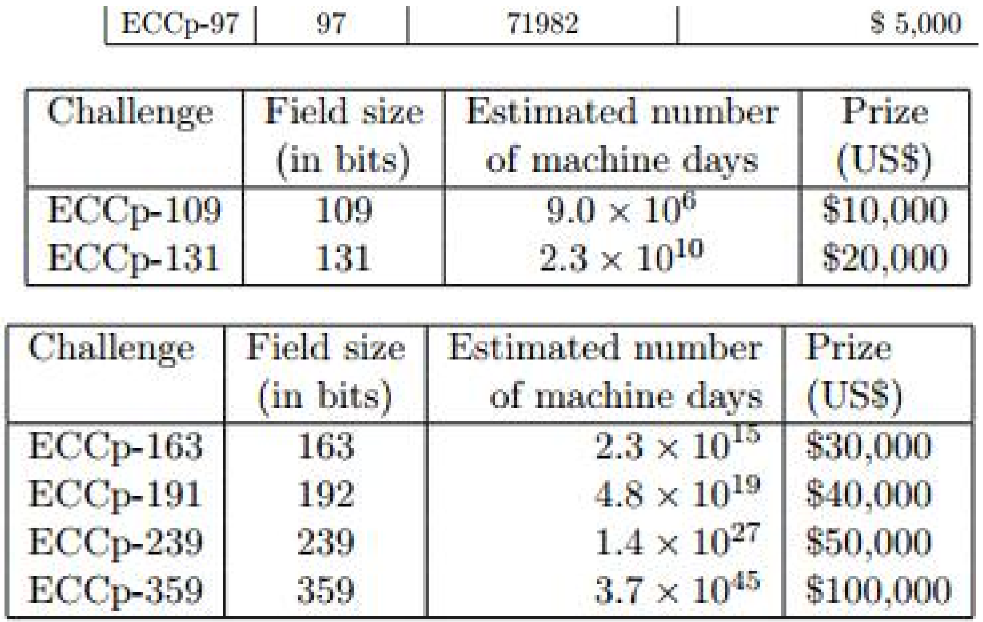
ECC - Certicom Challenges [1997, revised 2009]



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

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

Koblitz citation:

"Once I heard a speaker from NSA complain about university researchers who are cavalier about proposing untested cryptosystems. He pointed out that in the real world if your cryptography fails, you lose a million dollars or your secret agent gets killed.

In academia, if you write about a cryptosystem and then a few months later find a way to break it, you've got two new papers to add to your résumé!"

Neal Koblitz,
Notices of the American Mathematical Society,
September 2007.

Official Bitcoin Wiki

https://en.bitcoin.it/wiki/Myths#Bitcoins_are_worthless_because_they.27re_based_on_unproven_cryptography

“SHA256 and ECDSA which are used in Bitcoin are well-known industry standard algorithms. SHA256 is endorsed and used by the US Government and is standardized (FIPS180-3 Secure Hash Standard).

If you believe that these algorithms are untrustworthy then you should not trust Bitcoin, credit card transactions or any type of electronic bank transfer.”

Bitcoin has a sound basis in well understood cryptography.

Official Bitcoin Wiki

https://en.bitcoin.it/wiki/Myths#Bitcoins_are_worthless_because_they.27re_based_on_unproven_cryptography

"SHA256 and ECDSA which are used in Bitcoin are well-known industry standard algorithms. SHA256 is endorsed and used by the US Government and is standardized (FIPS180-3 Secure Hash Standard).

If you believe that these algorithms are untrustworthy then you should not trust Bitcoin, credit card transactions or any type of electronic bank transfer."

Bitcoin has a sound basis in well understood cryptography.

Well…actually it has major bug in it.

⇒ Major security scandal in the making?

⇒ Expect a lawsuit??? for

- failing to adopt the crypto/industry best practices,
- for supporting a dodgy cryptography standard,
- not giving users worried about security any choice,
- and lack of careful/pro-active/ preventive security approach etc...

Blame Satoshi ☺

Officially Not Recommended

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

Bitcoin EC

Base field = F_p with 256-bit prime $p = 2^{256}-2^{32}-977$

The curve equation is $y^2 = x^3+7 \bmod p$.

Special Multiples

Like “shortcuts in space”.

Fact: for the bitcoin elliptic curve
there exists SOME
special multiples (2 major ones in bitcoin)
such that:

$$\lambda * (x, y) = (\zeta * x, y)$$

3000 of μs in general
100 μs in bitcoin

5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd73

0.2 μs general curve
0.04 μs bitcoin

7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ef

ECDL Problem in Less Than Sqrt Time?

Yes, cf.

https://ellipticnews.wordpress.com/2016/04/07/ecdlp-in-less-than-square-root-time/

- For example if many users use the same curve [Pollard Rho NSA-style pre-computation attacks with low storage].
- Solving Semaev-style polynomial equations:
  - a lot of research on this topic recently,
    - including our own eprint.iacr.org/2006/003 paper.
  - most works however are in extension fields.
    - what about prime fields???

Recent Research on ECDL Problem

Christophe Petit, Michiel Kosters and Ange Messeng:

Algebraic approaches for the Elliptic Curve Discrete Logarithm Problem over prime fields, in PKC 2016, Springer.

First paper in years which attempts to solve ECDLP in mod P curves –curves used by hundreds of millions of people every day.

Some curves seem MORE vulnerable than other:

- NIST P-224

  $p-1 = 2^{96} * 3 * 5 * 17 * 257 * 641 * 65537 * 274177 * 6700417 * 67280421310721$

What About Bitcoin EC?

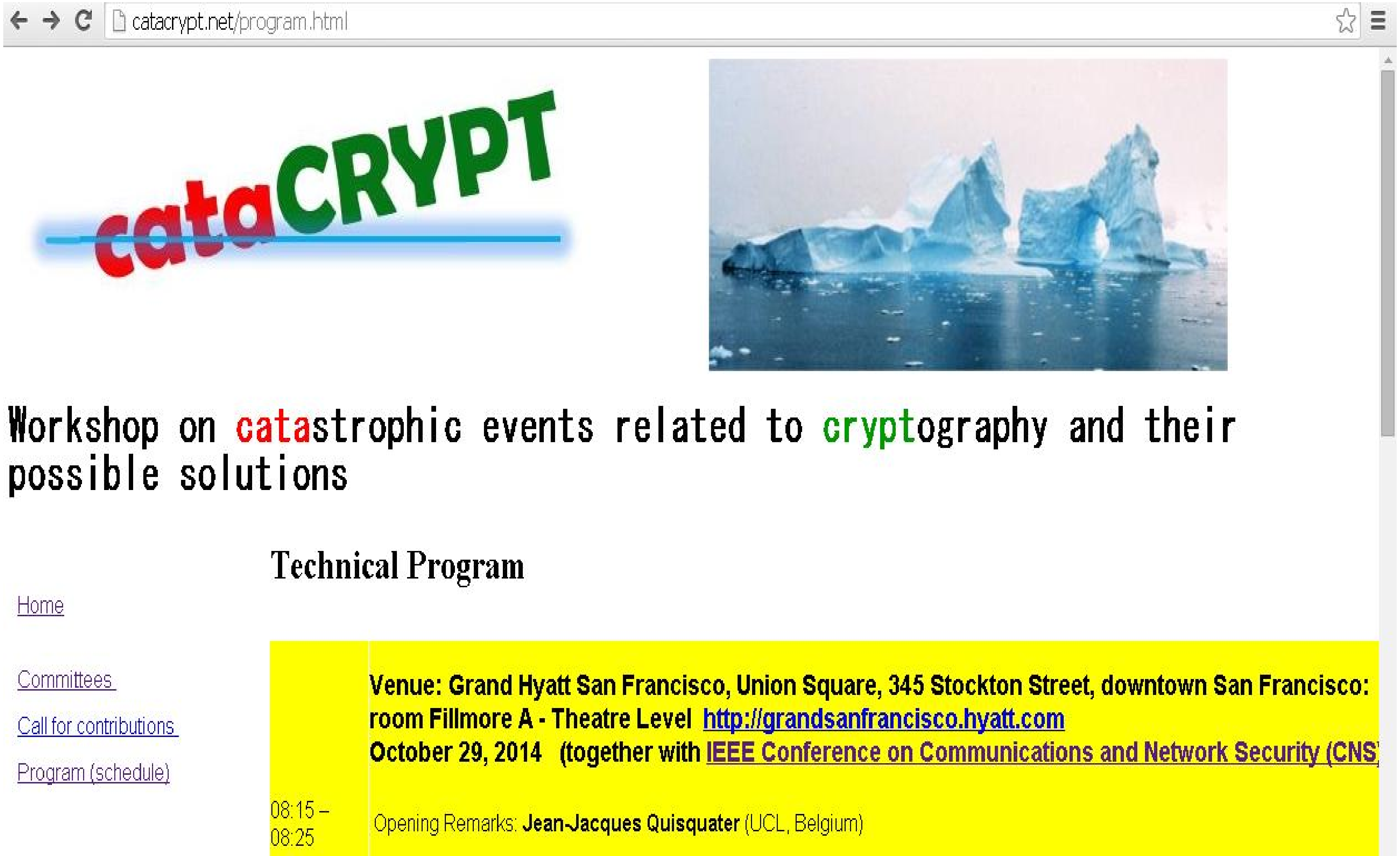
Base field = F_p with 256-bit prime $p = 2^{256}-2^{32}-977$

Fact: $p-1 = 2 * 13 * 80014349117 *$
$177349281343334057644417877 *$
$42802479871872742778975467705801408243$

So what???

So far no serious threats from this side.
But it is important to follow the ECC research.

What If? CataCrypt Conference



Workshop on catastrophic events related to cryptography and their possible solutions

Technical Program

Home

Committees

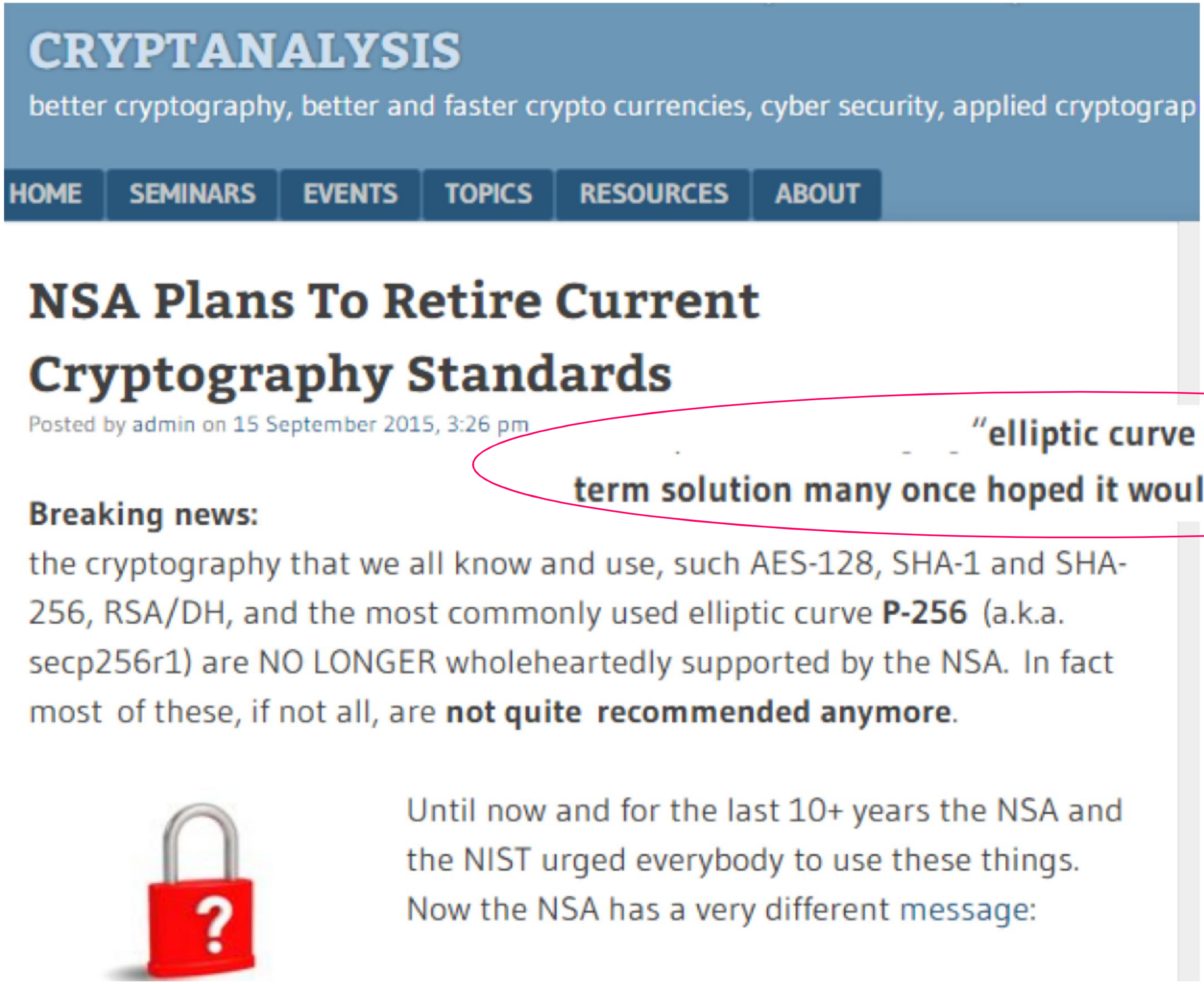
Call for contributions

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)

NSA Withdraws ECCs [Sept 2015]

http://blog.bettercrypto.com/?p=1917



CRYPTANALYSIS

better cryptography, better and faster crypto currencies, cyber security, applied cryptograp

NSA Plans To Retire Current Cryptography Standards

Posted by admin on 15 September 2015, 3:26 pm

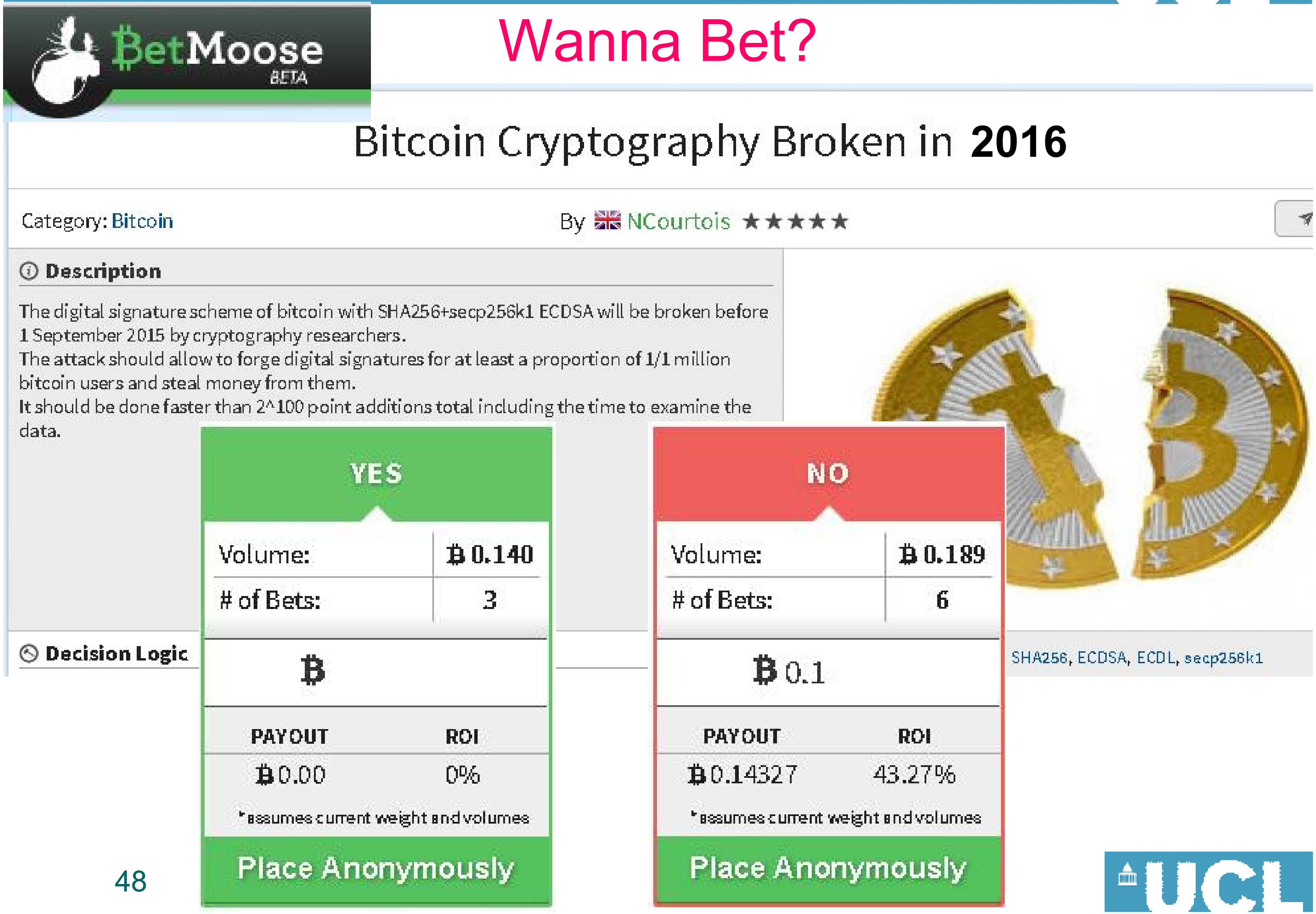
“**elliptic curve** cryptography is **not the long term solution many once hoped it would be**“.

Breaking news:

the cryptography that we all know and use, such AES-128, SHA-1 and SHA-256, RSA/DH, and the most commonly used elliptic curve **P-256** (a.k.a. secp256r1) are NO LONGER wholeheartedly supported by the NSA. In fact most of these, if not all, are **not quite recommended anymore**.

Until now and for the last 10+ years the NSA and the NIST urged everybody to use these things. Now the NSA has a very different message:

Wanna Bet?



Bitcoin Cryptography Broken in **2016**

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

Solutions

- Use each fresh bitcoin account only once!

- Satoshi did sth really brilliant:
  - Most transactions do NOT reveal the public key.

  - full disclosure is BAD security engineering and BAD security management…

Master Thesis Research Prize Fund 2016

For students doing research on blockchain security.

- Self-funded grassroots initiative:
  - – Independent from special interest groups.

Master Thesis Research Prize Fund 2016

UCL Finyear

clearmatics BLOCKCHAIN

TRAMONEX complymatic

Ethics: Cash prizes of moderate size.

=>demonstrate the honest effort of researchers in order to discover security vulnerabilities in bitcoin and blockchain systems
and in order to increase the awareness about potential and real attacks on these systems.

Master Thesis Research Prize Fund 2016

Prize Jury:

- **Prof. Jan Aldert Bergstra, Institute of Informatics, University of Amsterdam**
- **Prof. Alex Biryukov, University of Luxembourg**
- **Dr. Nicolas T. Courtois, Senior Lecturer, University College London**
- **Ass. Prof. Stefan Dziembowski, University of Warsaw, Poland**
- **Prof. Jean-Paul Delahaye, Lille University of Science and Technology, France**
- **Dr. Aggelos Kiayias, National and Kapodistrian University of Athens, Greece**
- **Prof. David Naccache, Ecole Normale Supérieure and Ingenico Labs, France**
- **Dr. Paolo Tasca, Deutschebank, Frankfurt, Germany**

Blockchain Anonymity

Privacy/Anonymity is NOT a concern for the 90%.

⇒ WRONG: this why we are losing this planet
to the corrupted criminal minority.

- **Asymmetry of information**
- **Market manipulation and big data**
- **You are no longer a customer, you are a slave**
- **Uberization and destruction of our economy:**
  - **export profits to offshore entities.**

Blockchain technology WILL NEVER be adopted by banks if it INCREASE the disclosures => need for anonymity solutions.

- **Ring signatures.**
- **Zero knowledge proofs.**
- **Other advanced crypto techniques which are POORLY studied.**

We will award cash prizes to students!

First awards in October 2016

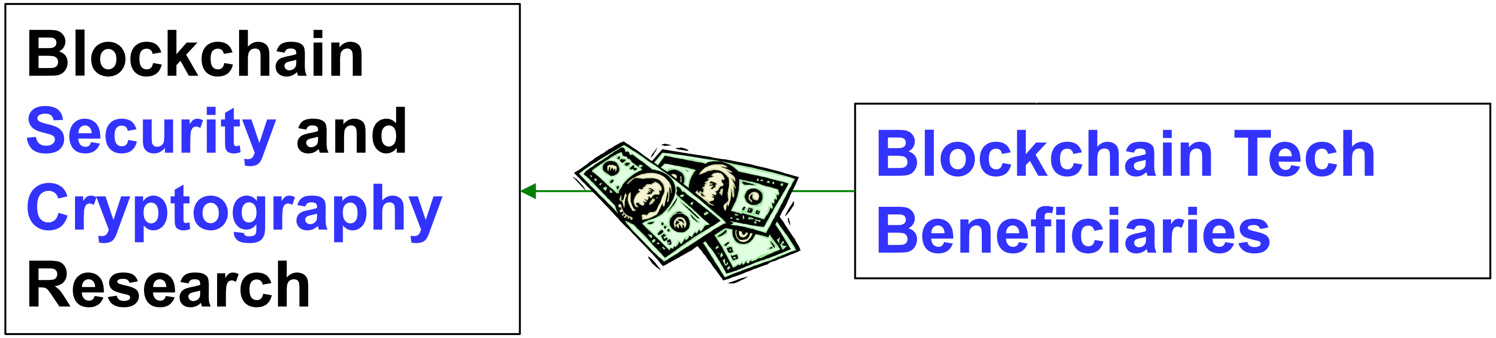
- **Master thesis and other research work.**

Examples:

- **5 BTC for a contribution to security of bitcoin/blockchain in a Master thesis/student work.**
- **5 BTC for discovery of attacks bugs or flaws in ZK proofs, ring signatures, ECCs, key management and other advanced cryptographic techniques relevant to blockchain tech.**

Sponsors needed!

Contact:
N.Courtois@cs.ucl.ac.uk



Blockchain Security and Cryptography Research

Blockchain Tech Beneficiaries