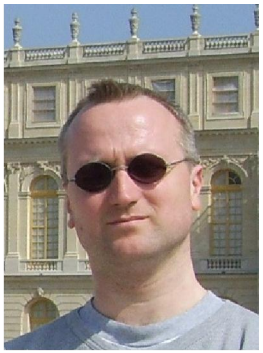
Bitcoin Storage Security Survey: Wallets Cold Storage BIP032

Nicolas T. Courtois

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

Dr. Nicolas T. Courtois

1. cryptologist and codebreaker



UNIVERSITY CIPHER CHAMPION

March 2013

Cyber Security Challenge UK

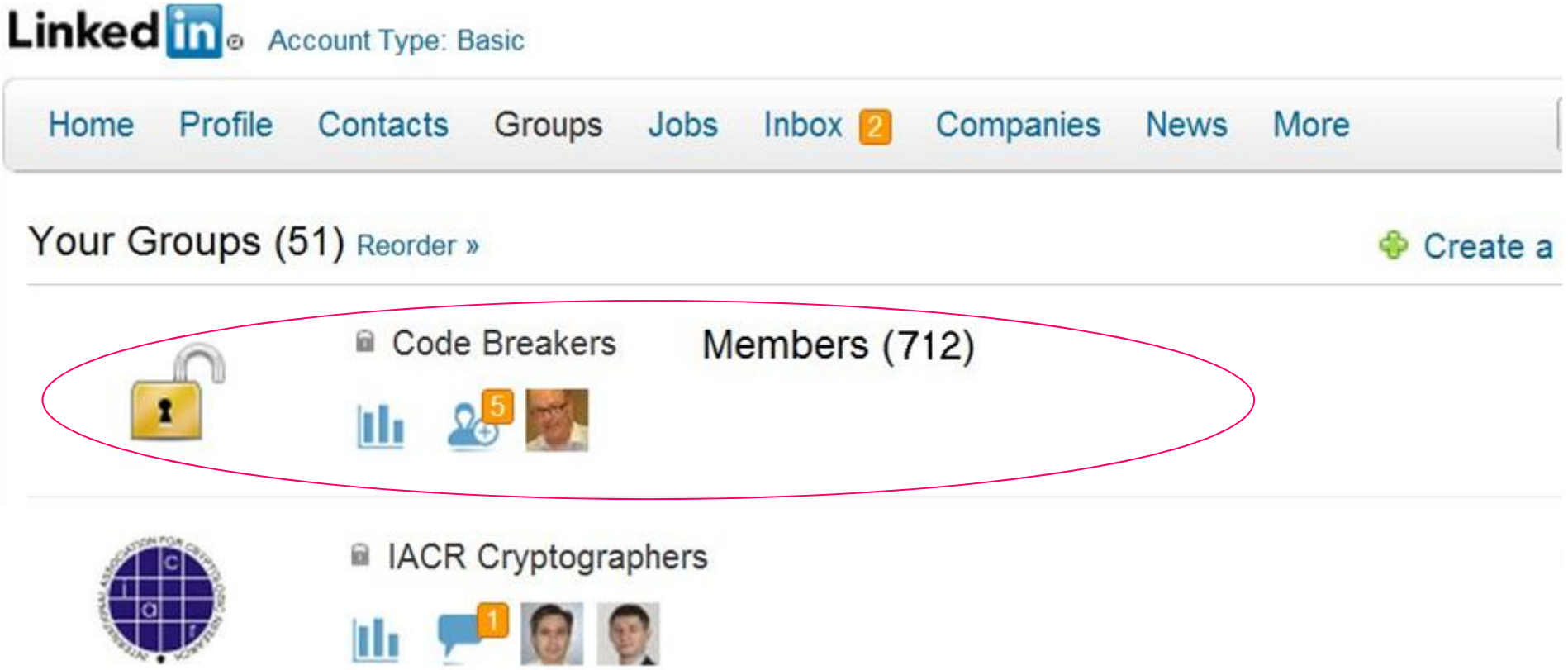
2. payment and smart cards (e.g. bank cards, Oyster cards etc…)

Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

LinkedIn


LinkedIn
Account Type: Basic
Home
Profile
Contacts
Groups
Jobs
Inbox 2
Companies
News
More
Your Groups (51)
Reorder »
Create a
Code Breakers
Members (712)
5
IACR Cryptographers
1

UCL Bitcoin Seminar

research seminar

=>In central London, runs EVERY WEEK!

public web page:

blog.bettercrypto.com / SEMINAR

or Google "UCL bitcoin seminar"

My Whole Life:

Tried to educate people about security…

My Whole Life:

Tried to educate… AND frequently FAILED…

My Whole Life:

Crying Wolf!

51%, Elliptic Curve, OpenSSL...

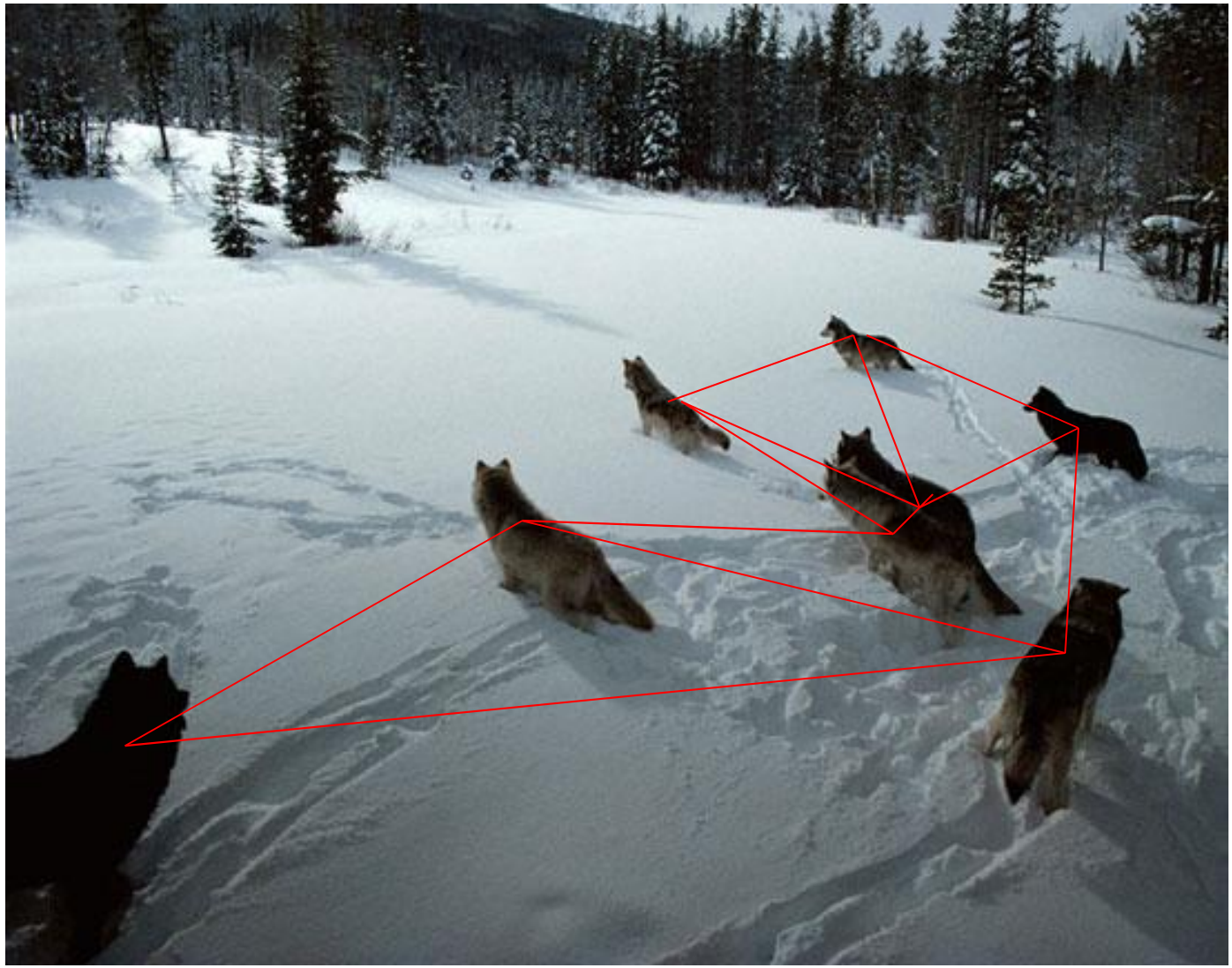
It did NOT help,

The Wolf was allowed to operate

We failed to protect our DATA

We failed to protect our MONEY

Solution = Decentralized P2P



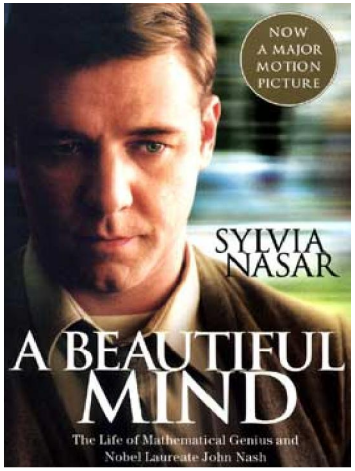
Solution = BlockChain

- Until recently, we've needed central bodies – banks, stock markets, governments, police forces – to settle vital questions.
  - Who owns this money?
  - …
  - Now we have a small piece of […] computer code that will allow people to solve the thorniest problems without reference to "the authorities".

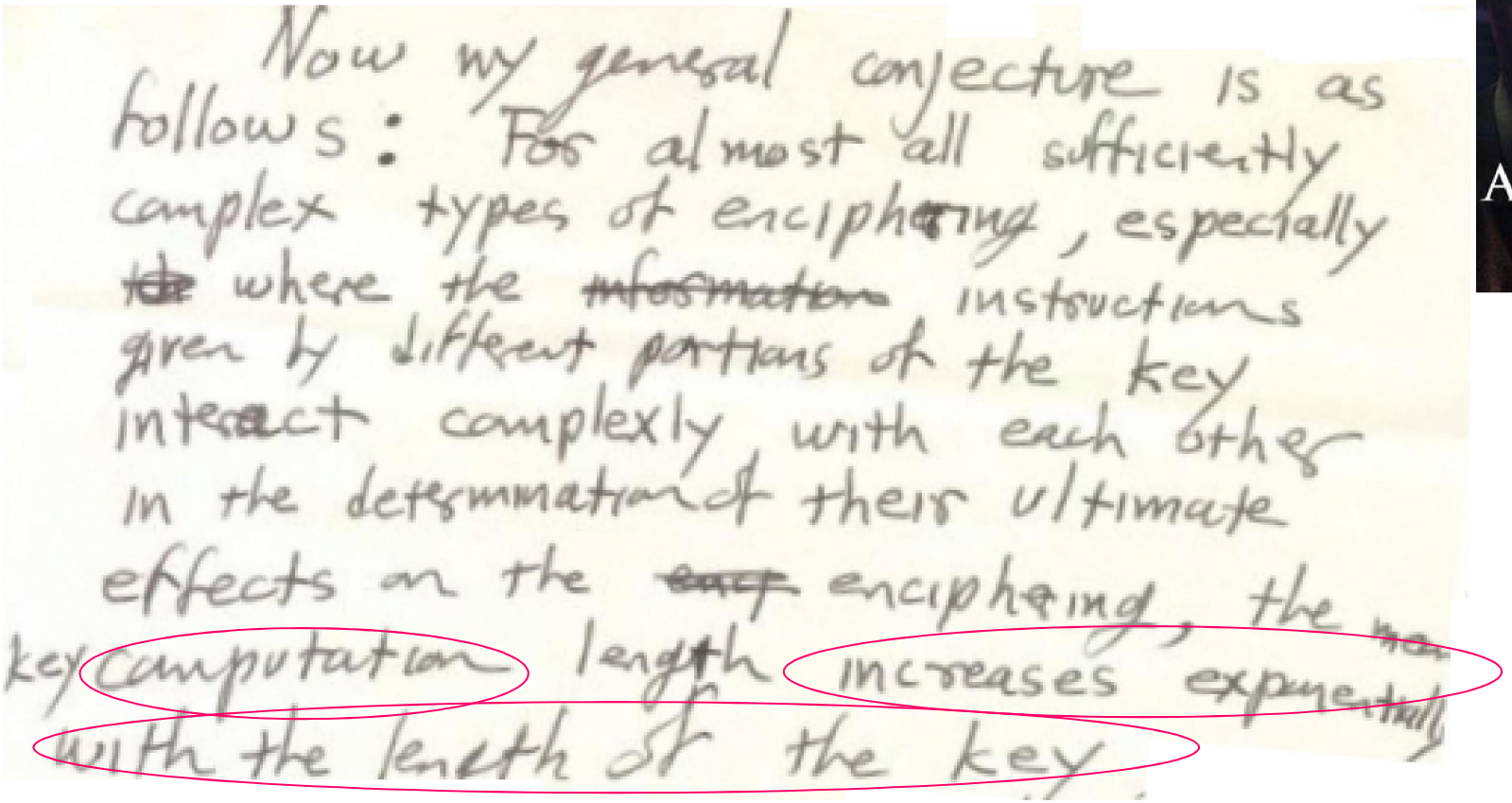
http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html
[11 June 2014]

The Telegraph
The coming digital anarchy

John Nash - 1955



In 2012 the NSA declassified his hand-written letter:

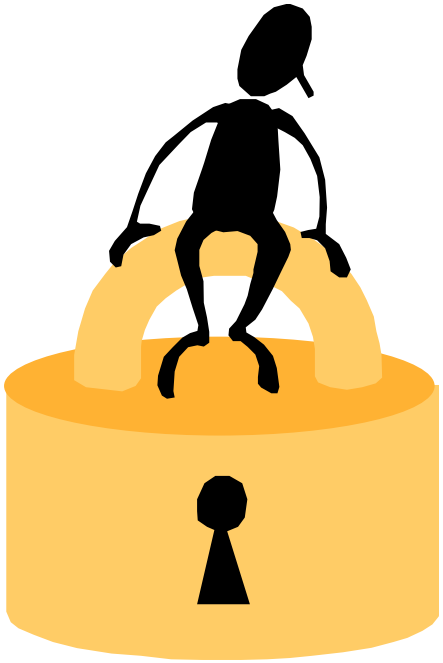

Now my general conjecture is as follows: For almost all sufficiently complex types of enciphering, especially where the ~~information~~ instructions given by different portions of the key interact complexly with each other in the determination of their ultimate effects on the ~~encip~~ enciphering, the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

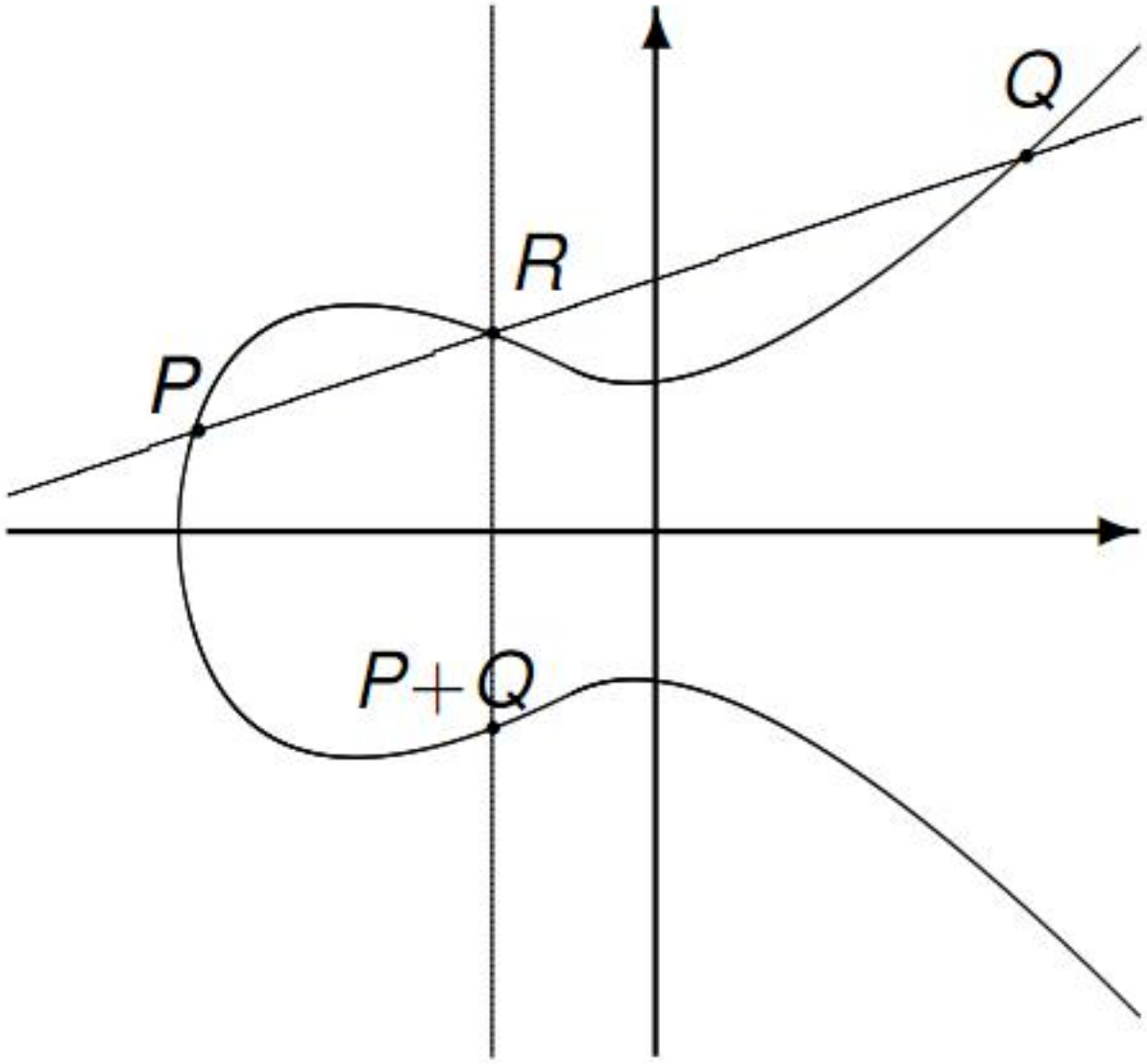
He also says that:

[…] 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

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 3 BILLION $.

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

UCL

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?

BetMoose BETA

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:	Ƀ 0.140
# of Bets:	3

Ƀ

PAYOUT	ROI
Ƀ 0.00	0%

*assumes current weight and volumes

Place Anonymously

NO	
Volume:	Ƀ 0.189
# of Bets:	6

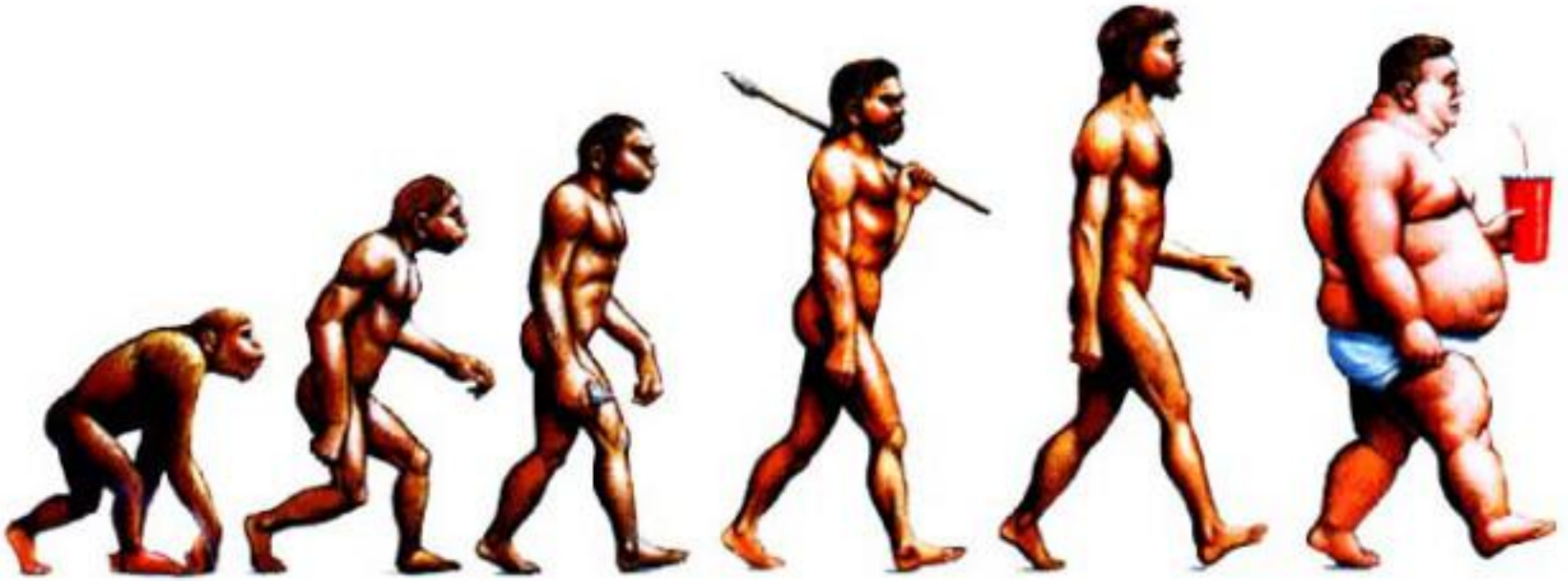
Ƀ 0.1

PAYOUT	ROI
Ƀ 0.14327	43.27%

*assumes current weight and volumes

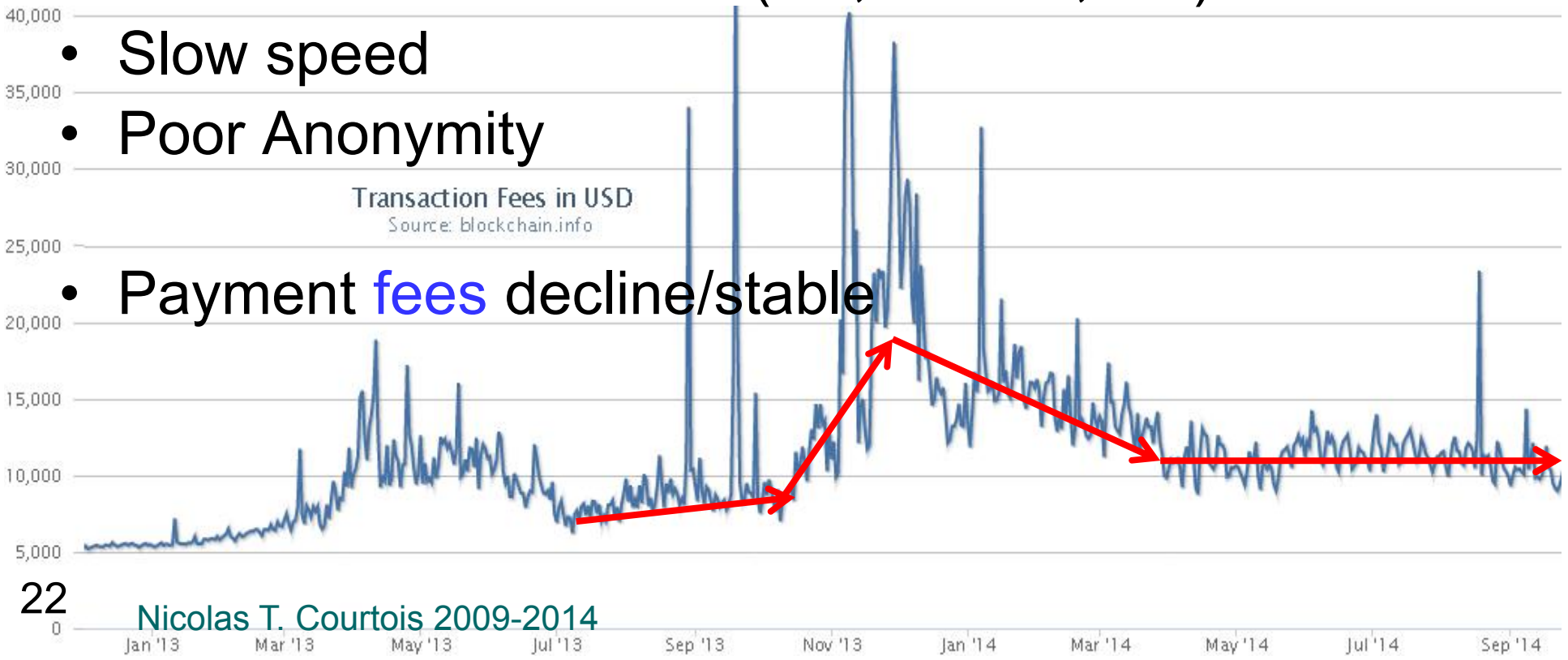
Place Anonymously

Is Bitcoin Improving?



Bitcoin Troubles

- Crypto gets broken?
- Monetary policy: genius, weird or mad?
- 51% attacks and double spending: easy!
- P2P network in decline (XX,000=>5,000)
- Slow speed
- Poor Anonymity
- Payment fees decline/stable



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]

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

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 alt-coins.

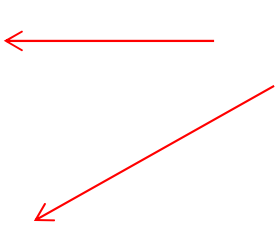
Bitcoin vs.

Security Engineering

Re-Engineering Bitcoin:

We postulate:

1. Open design.



[Saltzer and Shroeder 1975]

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).

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!

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. Who can force companies to publish their specs???

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)

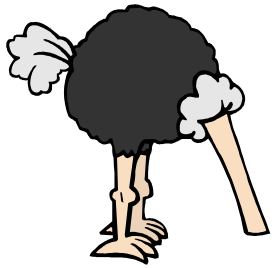
Prevent the erosion of profitability / barriers for entry for competitors / "inimitability"

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)

- Full disclosure for public keys is unbelievably stupid…
  - cf. next slide!

Do NOT Disclose Public Keys!

- Full disclosure for public keys is 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!
  - it does solve the problem raised by Diffie at CataCrypt in San Francisco:
    HOW DO YOU PROTECT AGAINST UNKNWOWN ATTACKS?

CataCrypt Conference

catacrypt.net/program.html

cataCRYPT

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)

Breaking News

blog.bettercrypto.com

NSA Plans To Retire Current Cryptography Standards

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

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:

- There will be a transition to new crypto algorithms coming very soon.

Introducing Bitcoin

Bitcoin In A Nutshell

- bitocoins are cryptographic tokens, binary data = 01010011010101010…
  - stored by people on their PCs or mobile phones
- ownership is achieved through digital signatures:
  - you have a certain cryptographic key, you have the money.
  - publicly verifiable, only one entity can sign

- consensus-driven, a distributed system which has no central authority
  - a major innovation: financial transactions CAN be executed and policed without trusted authorities.
  - bitcoin is a sort of financial cooperative or a distributed business.
- based on self-interest:
  - a group of some 100 K people called bitcoin miners own the bitcoin “infrastructure” which has costed > 1 billion dollars (my estimation)
  - they make money from newly created bitcoins and fees
  - at the same time they approve and check the transactions.
  - a distributed electronic notary system

Two Key Concepts

- initially money are attributed through **Proof Of Work (POW)** to one public key A
  - to earn bitcoins one has to “work” (hashing) and consume energy (pay for electricity)
  - now in order to cheat one needs to work even much more (be more powerful than the whole network), more precisely:

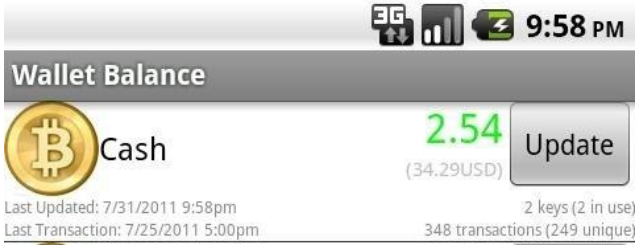
- money transfer from public key A to public key B:
  - **like signing a transfer in front of one notary which confirms the signature**,
  - multiple confirmations: another notary will re-confirm it, then another, etc…
  - we do NOT need to assume that ALL these notaries are honest.
    - at the end it becomes too costly to cheat

In Practice


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

Wallets

- Wallet: file which stores your “money".
- A Bitcoin client App
  is also called a wallet



Digital Currency

Bitcoin is a
=>PK-based Currency:

– bank account = a pair of public/private ECDSA keys

– spend money = produce a digital signature

Main Problem:

Bitcoins can be “spent twice”.

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

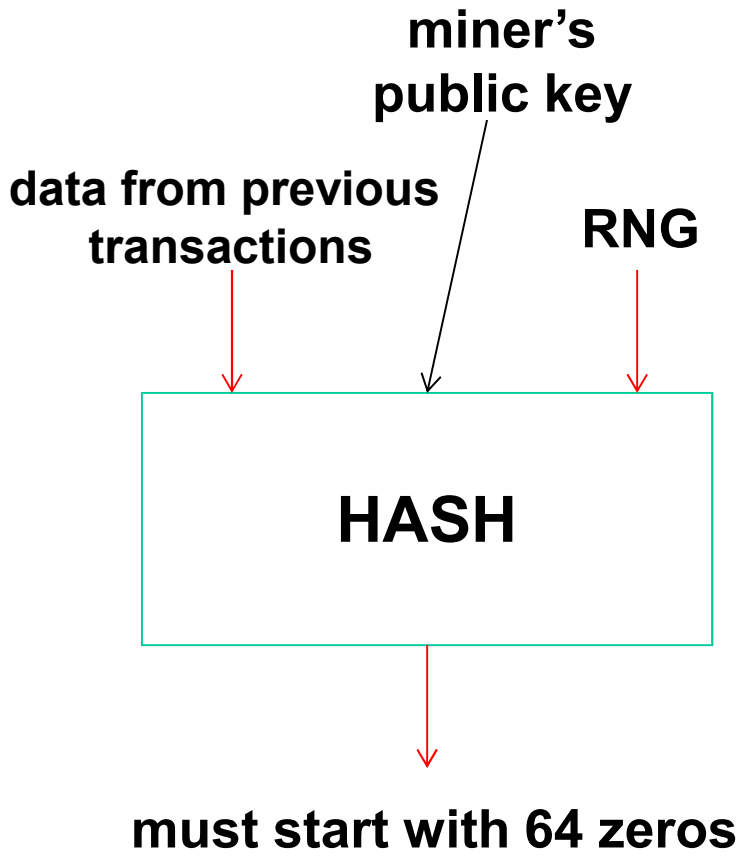
Block Chain

Bitcoin Mining

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

Ownership:

– "policed by majority of miners":



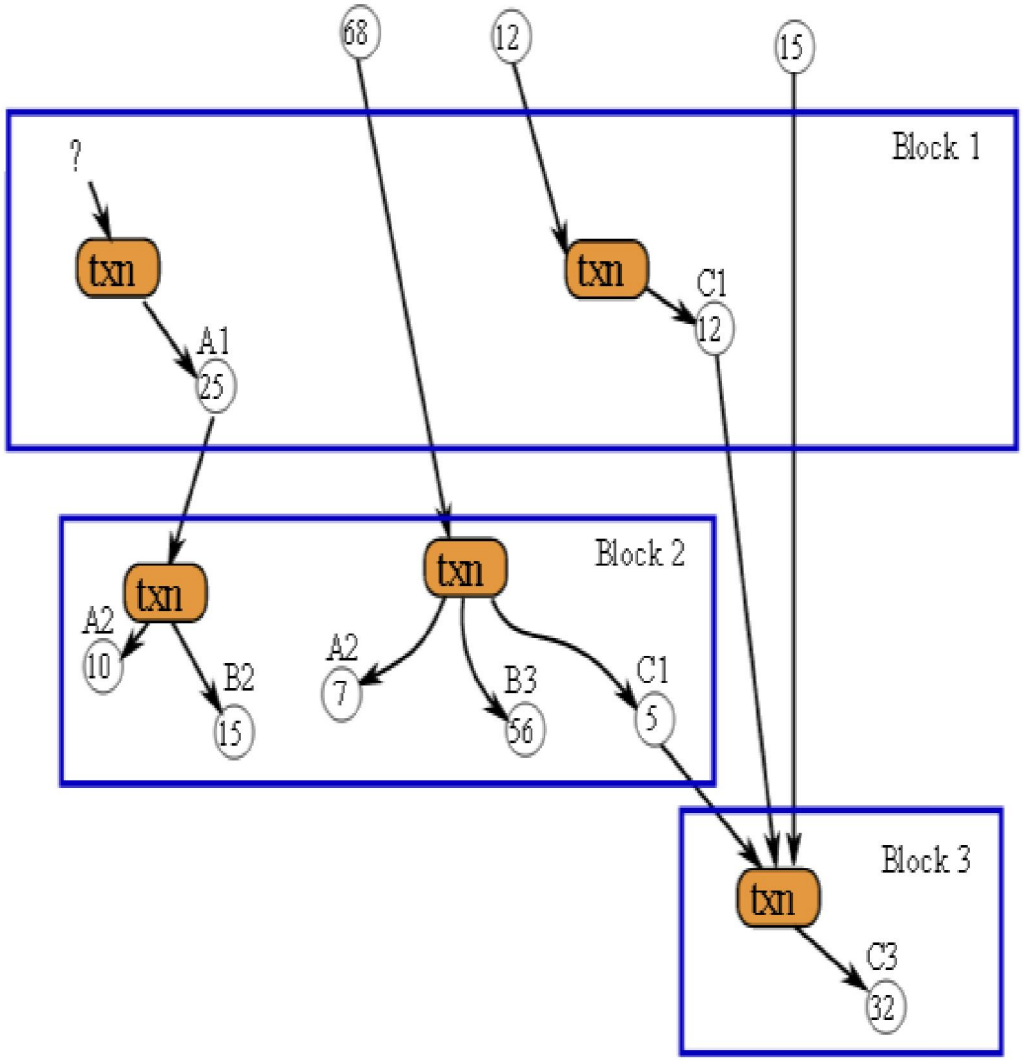
Block Chain

Def:

A transaction database shared by everyone.

Also a ledger.

Every transaction since ever is public.

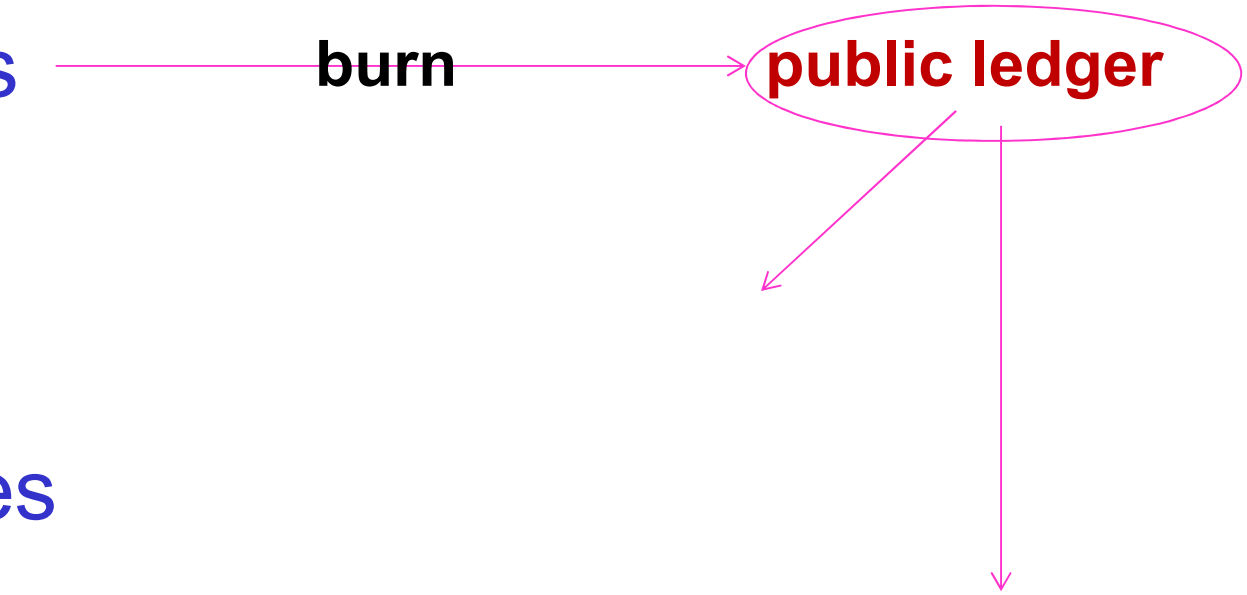


Tx LifeCycle

- Miner nodes
- Peer Nodes
- Wallet Nodes

tx

tx



Bitcoin Address

Ledger-Based Currency

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

Reamrks:

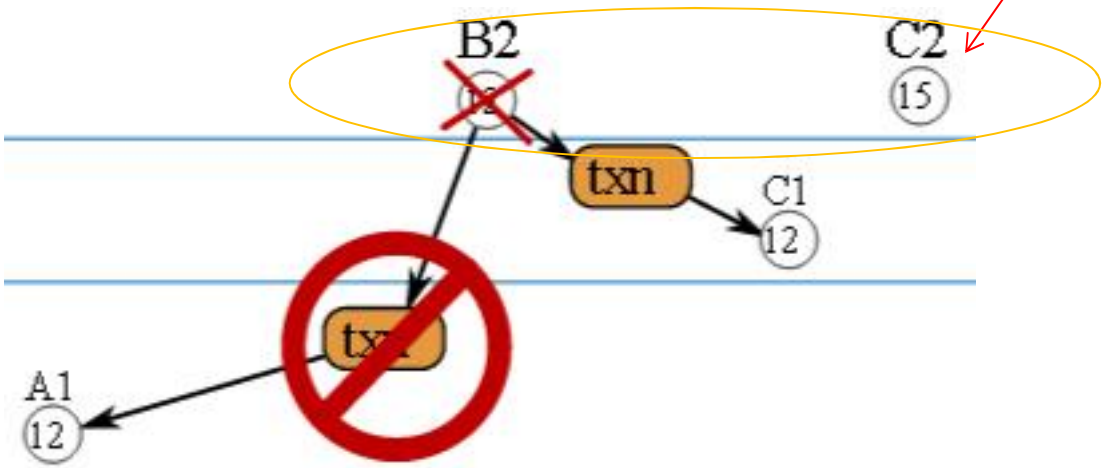
- PK is NOT public!
- only H(public key) is revealed!
- PK remains confidential until some money in this account is spent.
- SK = private key: always keep private, allows transfer of funds.

Bitcoin Ownership

Amounts of money are attributed to public keys.

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

Destructive, cannot spend twice:



*Multi-Signature Addresses

MultiSig = Addresses Starting with 3

Bitcoin can require simultaneously several private keys, in order to transfer the money.

- For example 2 out of 3 signatures are required to spend bitcoins.
- The keys can be stored on different devices (highly secure).
- Can work without backups: if one device is lost, use other devices to transfer bitcoins to a new multisig address with another set of devices...

Multi-Sig Concept is NOT new…

1993

Efficient multi-signature schemes for cooperating entities

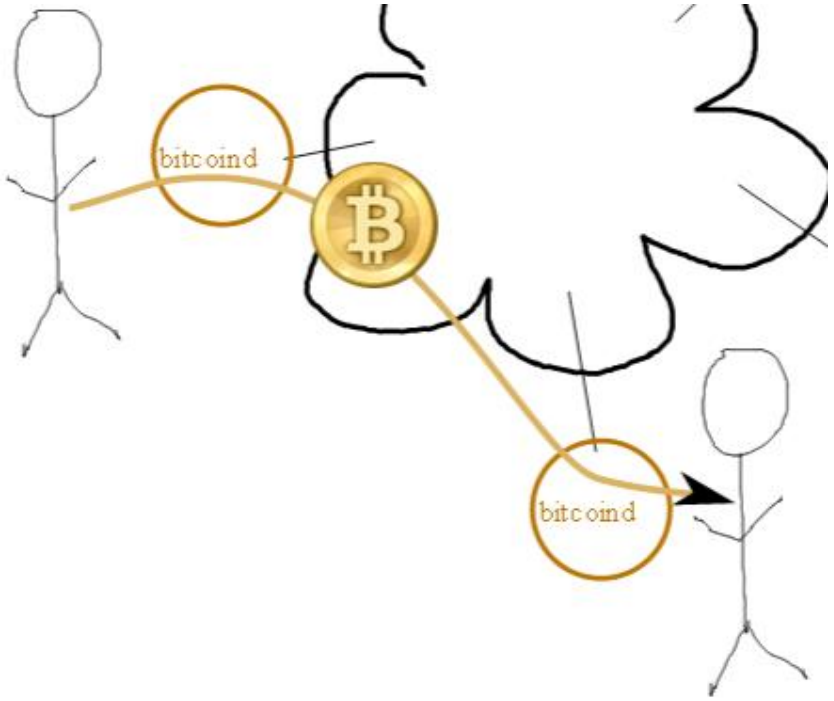
Olivier Delos [1] and Jean-Jacques Quisquater [2]

1983

K. Itakura, K. Nakamura:
A public-key cryptosystem suitable for digital multi-signatures

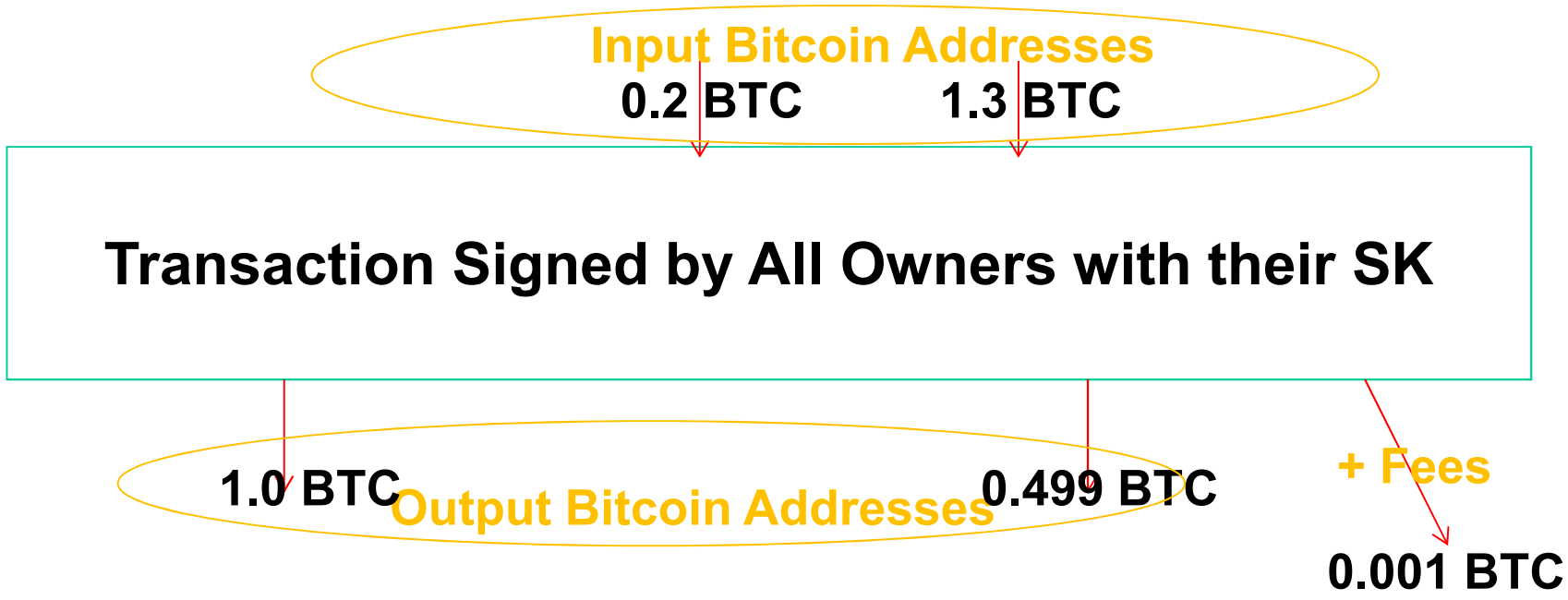
BTC Transfer

To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36
Amount: 1.0 BTC
SEND



Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



Transaction Scripts

Signed Tx / Final Tx

byte by byte (similar but not identical to raw blocks seen before)
(this is done twice, with different scriptSig)

version		01 00 00 00
input count		01
input	previous output hash (reversed)	48 4d 40 d4 5b 9e a0 d6 52 fc a8 25 8a b7 ca a4 25 41 eb 52 97 58 57 f9 6f b5 0c d7 32 c8 b4 81
	previous output index	00 00 00 00
	script length	**scriptSig length 1 byte**
	scriptSig	script containing signature **scriptSig**
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00
	script length	**scriptPubKey length 1 byte**
	scriptPubKey	script containing destination address **scriptPubKey**
block lock time		00 00 00 00 **(not widely used)**

2 scripts

Second scriptSig

sign+PKey

len= 1+71+ 1+65 = 138 BUT NOT ALWAYS!

scriptSig

PUSHDATA 47		47
signature (DER)	sequence	30
	length	44
	integer	02
	length	20
	X **r**	2c b2 65 bf 10 70 7b f4 93 46 c3 51 5d d3 d1 6f c4 54 61 8c 58 ec 0a 0f f4 48 a6 76 c5 4f f7 13
	integer	02
	length	20
	Y **s**	6c 66 24 d7 62 a1 fc ef 46 18 28 4e ad 8f 08 67 8a c0 5b 13 c8 42 35 f1 65 4e 6a d1 68 23 3e 82
SIGHASH_ALL		01
PUSHDATA 41		41
public key	type	04
	X	14 e3 01 b2 32 8f 17 44 2c 0b 83 10 d7 87 bf 3d 8a 40 4c fb d0 70 4f 13 5b 6a d4 b2 d3 ee 75 13
	Y	10 f9 81 92 6e 53 a6 e8 c3 9b d7 d3 fe fd 57 6c 54 3c ce 49 3c ba c0 63 88 f2 65 1d 1a ac bf cd

scriptSig1
signature
(r,s)

scriptSig2
=Pkey
=(x,y)

Is Bitcoin Secure?

Satoshi claimed it is…

Wallets


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

Bottom Line

Main Functionality:

-Private Key Generation

-Export public key

-ECDSA sign

BTChip HW1

hardwarewallet.com

Ledger

ledgerwallet.com

-optional:

- sign full BTC transactions
- confirm recipient on the screen!

(huge classical pb with all smart cards and digital signature devices,
Ledger has a clever solution: regurgitates inputs on another device USB keyboa

Trezor

bitcointrezor.com

BTChip HW.1

since Jan 2013

Ledger HW.1

Visit website | Source code

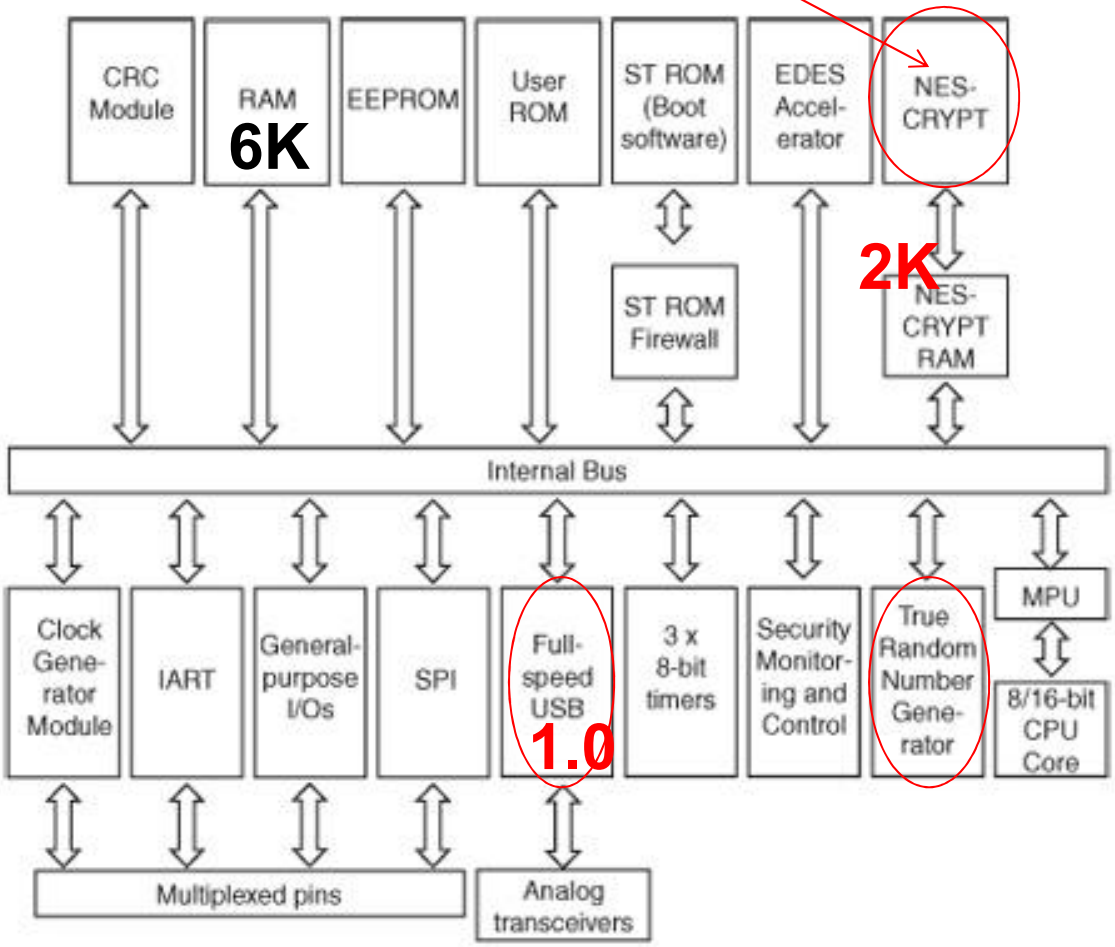
- Control over your money
- Variable validation
- New app
- Very secure environment
- Variable privacy

HW.1 is a hardware wallet built upon a ST23YT66 banking smartcard platform. It keeps the user private keys safe, validates transactions, can be used as a secure prepaid card or a multisignature party. While not open-source, it can be deterministically validated.

*Features of USB card ST23YT66

NESCRYPT crypto-processor for PK crypto

- 900 ms for 1 ECDSA signature
- 900 ms for key gen
- encrypts private keys on the card ('content' key) 3DES CBC
  - content key can be protected with "a GlobalPlatform Secure Channel" authentication mechanism



released March 2014 Trezor **by Satoshi Labs Prague, CZ**

+ display: know to whom you send the money!

+- has open source firmware: https://github.com/trezor/trezor-mcu

TREZOR

Visit website | Source code

Control over your money

Variable validation

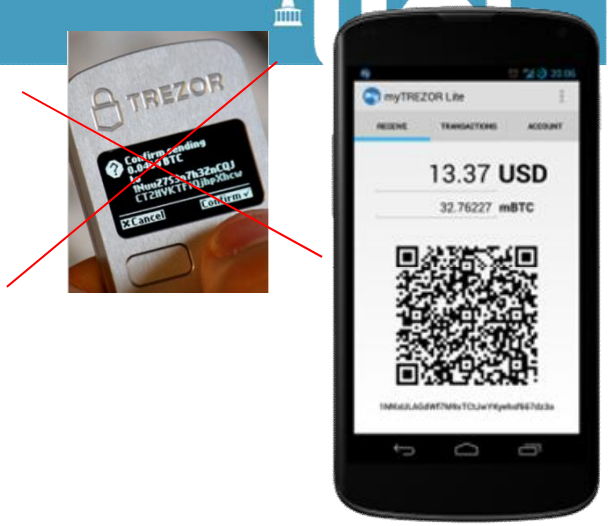
New app

Very secure environment

Variable privacy

TREZOR is a hardware wallet providing a high level of security without sacrificing convenience. Unlike cold storage, TREZOR is able to sign transactions while connected to an online device. That means spending bitcoins is secure even when using a compromised computer.

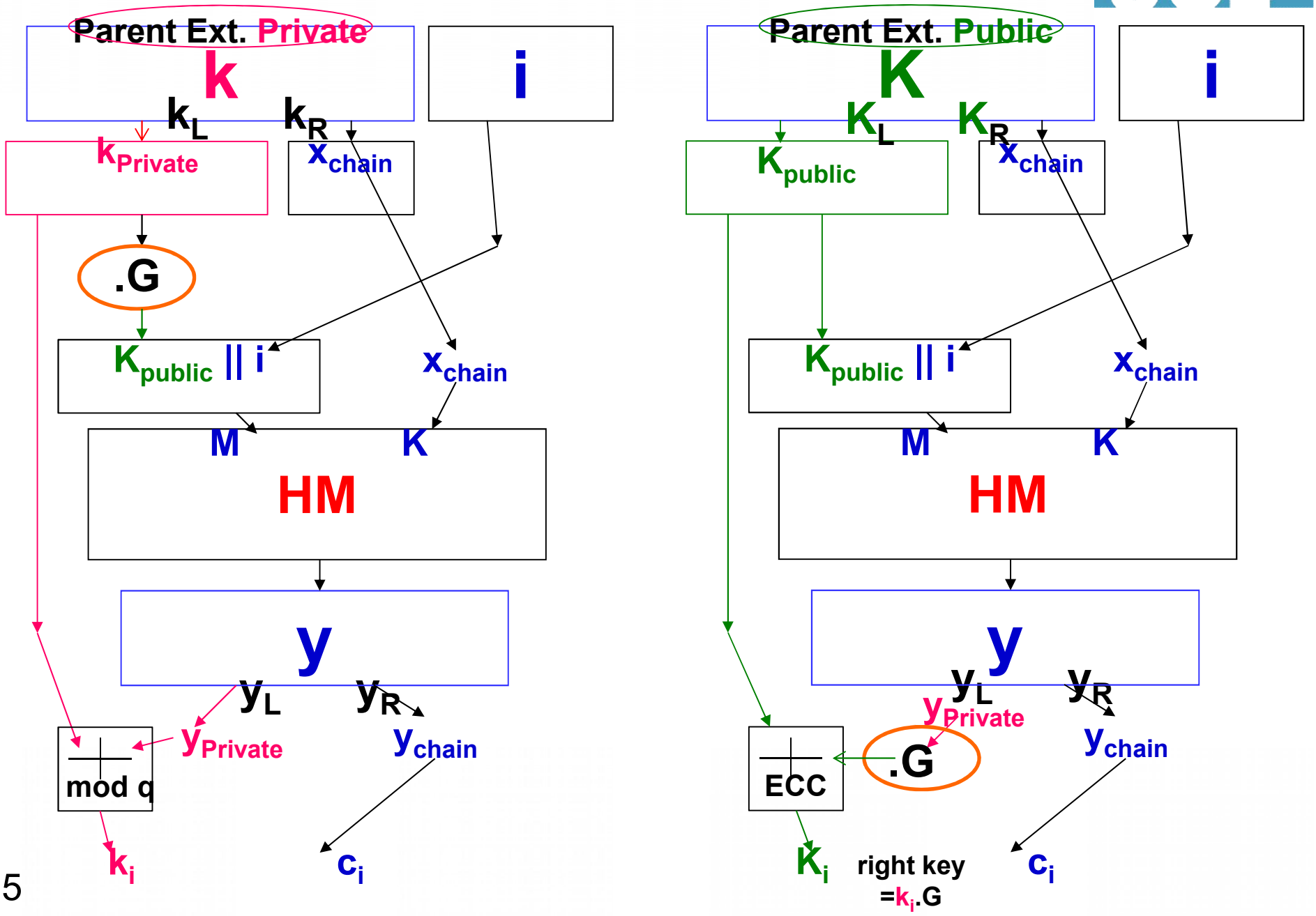
+ Trezor Lite App



Allows to see your money
when you don't have your device with you!

Based on BIP032 audit capability
=> quite dangerous: see

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


Parent Ext. Private
k
i
k_L
k_R
$k_{Private}$
x_{chain}
.G
K_{public} || i
x_{chain}
M
K
HM
y
y_L
y_R
$y_{Private}$
y_{chain}
mod q
k_i
c_i
Parent Ext. Public
K
i
K_L
K_R
K_{public}
x_{chain}
K_{public} || i
x_{chain}
M
K
HM
y
y_L
y_R
$y_{Private}$
y_{chain}
ECC
.G
k_i
right key
$=k_i.G$
c_i

Ledger

- have their own operating system!
  - closed source, their Chrome front-end is open source
  - due to the current JavaCard limitiation:
    - cannot implement deterministic ECDSA (RFC6979)
- bitcoin tx processing implemented inside (unlike HW.1)
  - claimed to be a “more secure” evolution of HW.1
- communicates with Google Chrome directly, no middleware
- data retention: 30 years
- open: no NDA for any wallet to support this

It Implements:

- Standard Multisig, P2SH style (BIP016)
- BIP032 : HD Wallets
  - ⇒ danger?, they have fixed it!
  - ⇒ solution: implements RFC 6979, deterministic signatures
- BIP039: seed mnemonic (list of words in English)
- BIP044: specific wallet structure

Security

- master backup
  - printed card with master private seed

  + long passhrase to be written on paper (used only to recover)
  - recovery also possibly if the hardware is lost
    - standard method BIP39, no lock-in, can be recovered on 3rd party soft/hard
  - enter wrong PIN 3 times=>all data are claimed to be erased
  - claimed totally anonymous
    - except browser IP address will be revealed when you send Tx to the network
- each device is paired with a printed card A=>3, to be kept with the wallet,
  - this card=second factor authn. (malware cannot use the device)
  - duo edition has the same card: can create 2 identical hardware wallets
  - Pb: PIN code is entered on a PC: BUT
    - to sign a transaction, need to enter correspondance codes A=>3 "based on a random sampling of the payment address"

CoinKite

- card + terminal with HSM

+ supports multisig

- Pb.
  - “each new member receives a "welcome email" which contains the "xpubkey" (extended public key) for their deposits.”
  - super dangerous!

Are Known Wallet Solutions Secure?

??

Incidents at Operation: Bad Randoms

Bad Randoms

First publicized by Nils Schneider:

28 January 2013

D47CE4C025C35EC440BC81D99834A624875161A26BF56EF
7FDC0F5D52F843AD1

$\Rightarrow$ repeated more than 50 times…

Used twice by the SAME user!

ECDSA Signatures

Let **d** be a private key, integer **mod n** = ECC [sub-]group order.

- Pick a random non-zero integer **0<a<n-1**.
- Compute **R=a.P**, where **P** is the base point (generator).
- Let **r** = $(a.P)_x$ be its x coordinate.
- Let **s = (H(m) + d*r) / a mod n** .

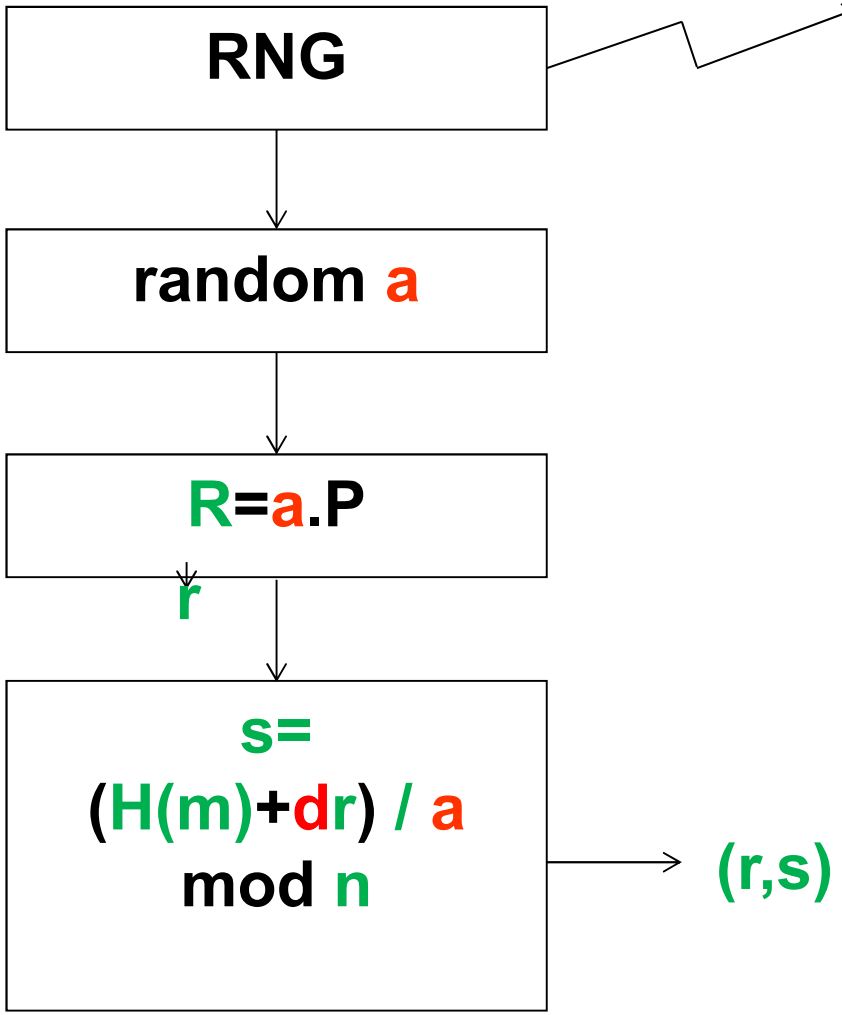
The signature of m is the pair **(r,s)**.

(512 bits in bitcoin)

Attack – 2 Users

has already happened 100 times in Bitcoin

random a: must be kept secret!



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

$(s_1a-H(m_1))/d_1 = r = (s_2a-H(m_2))/d_2 \bmod n$

=>

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

each person can steal the other person's bitcoins!

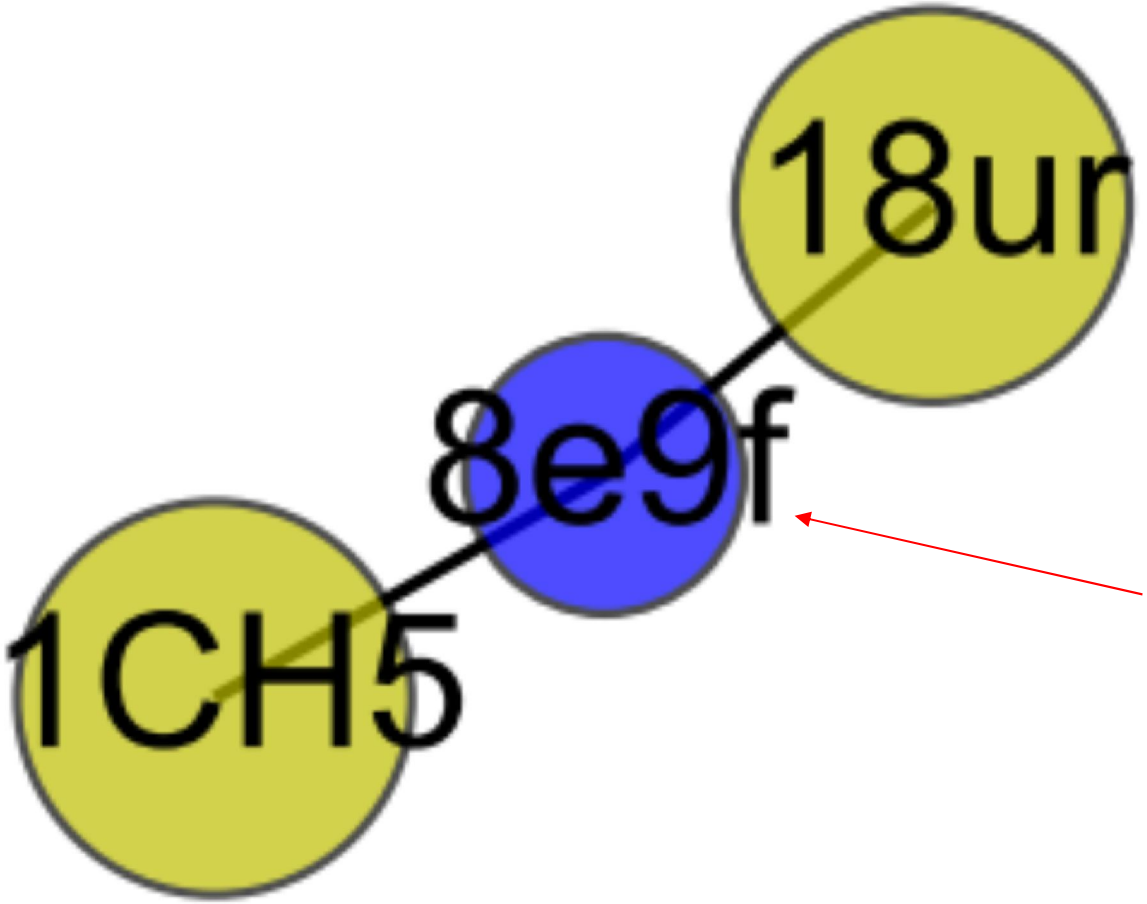
=>any of them CAN recompute k used

Our Graph Model

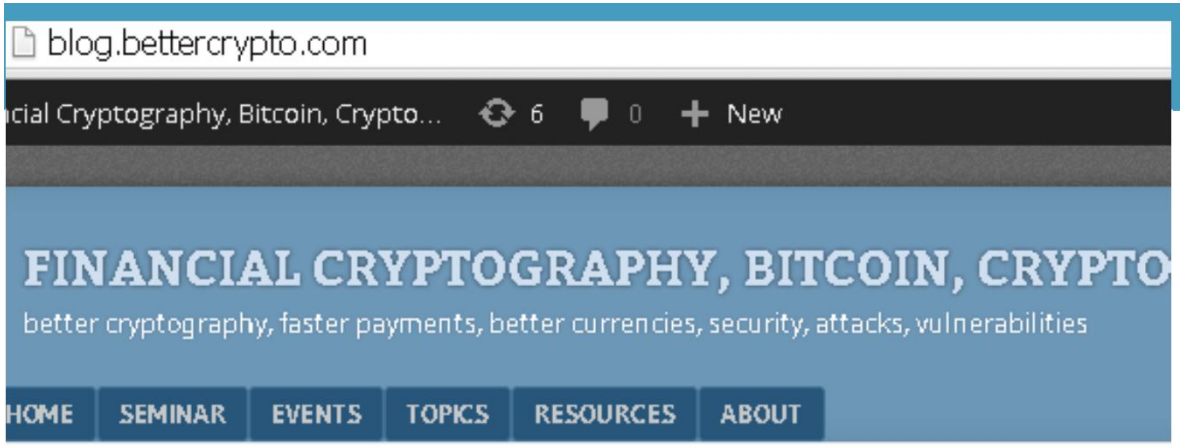
8e9fafd24f498744078c375b42ea087f5c43c8a5131949d1e19df32e0b4f9a67 2x 09Jan15-09Jan15

1x /1CH5R3DpWBgdbanQpHbJ8mtWCCWjHCx5ph 338168/tx533/i0

1x /18urmgKfTMC8AihEUzj7CpZfsxmg5ZUovE 338168/tx533/i1



2 users have used the same random



UCL

Our Online Database

9e199edb08bec948740e84cc6f91f0bbbfe36bc5f10546e0c1a6e2655f2c6019 4x 07Jan15-07Jan15

1x /1LR63Z94Lz29XVvnwaWi4JViREpFk4BFZf 337956/tx26/i3

1x /12rdRMTZQ6uuVucRnPtSmZRoqp2MVgBmh9 337956/tx26/i1

1x /1BPVuwza9pDHpbzUBMLUyhyV7PnuF2iJGx 337956/tx26/i2

1x /147rzbsdsqc2YKeGQRUs3jaCxyufVRz8Kh 337956/tx26/i0

c471b1ce535f6331d07759eeaafab4c1a276cdafa86245a7bf61f29236619367 7x 04Jan15-04Jan15

1x /1DDessF6x8s1RFN116aZ36PzVRRj5YUFA7 337458/tx25/i1

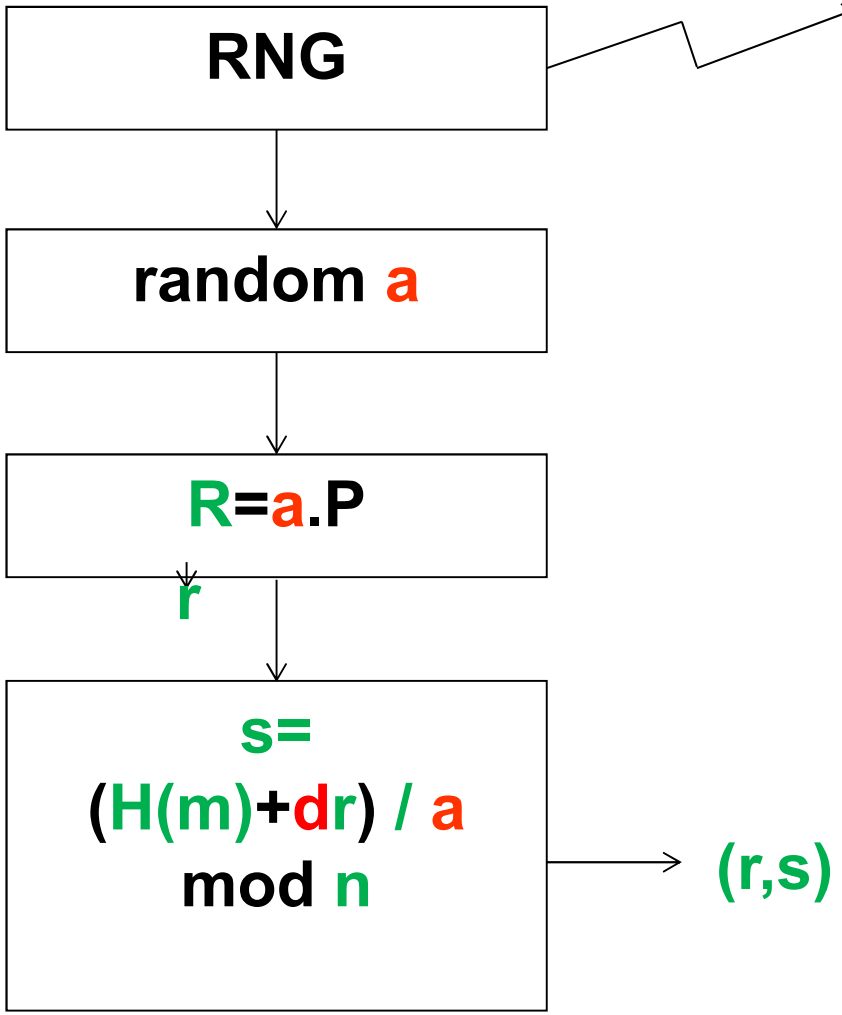
1x /1KdpXyEtFsr9Sugf3wo5bS9328y5cZ1oXK 337458/tx25/i0

1x /1GMu2kbqx8Y5ZLXkPfbVJzakddHo2Vjmde 337458/tx25/i5

1x /1KjLEUrdUiN7a2N6B8xY3V6bL1U1UJpCCA 337458/tx25/i2

Attack – Same User

random a: must be kept secret!



has also happened 100 times in Bitcoin

same a used twice by the same user (d_1=d_2). In this case we have: (s_1a-H(m_1)) = rd =
(s_2a-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

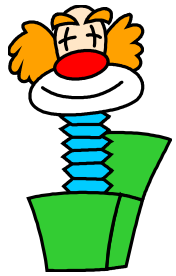
anybody can steal the bitcoins!

Have These Problems Stopped in 2013?

Lots of problems in May 2012, fixed.

2013: Android bug was fixed…

And then there was another MASSIVE outbreak…



And then another…

Dec. 2013

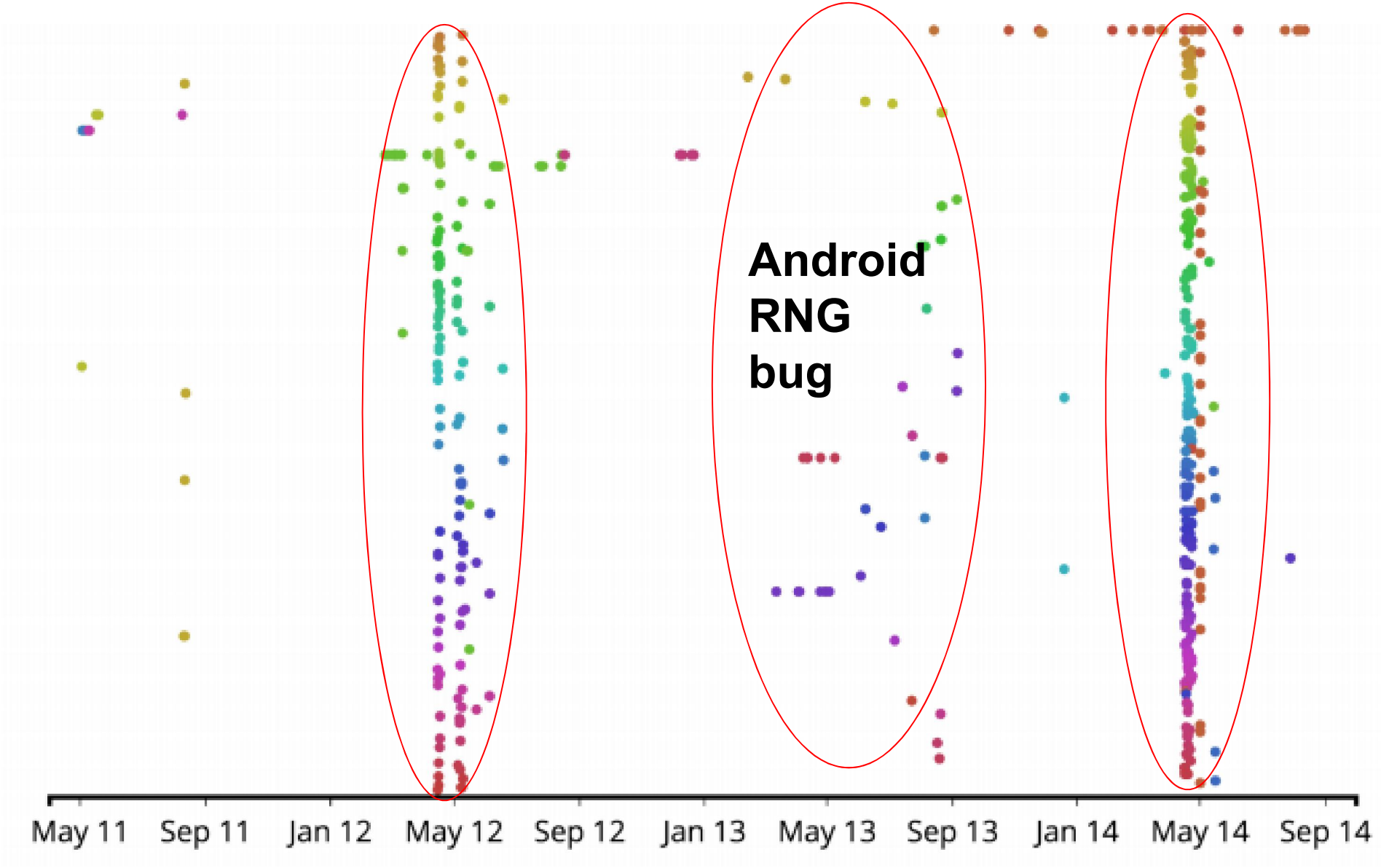
At 30C3 conference in Germany on 28 Dec 2013
Nadia Heninger have reported that they have identified
a bitcoin user on the blockchain
which has stolen some 59 BTC due to
these bad randomness events,

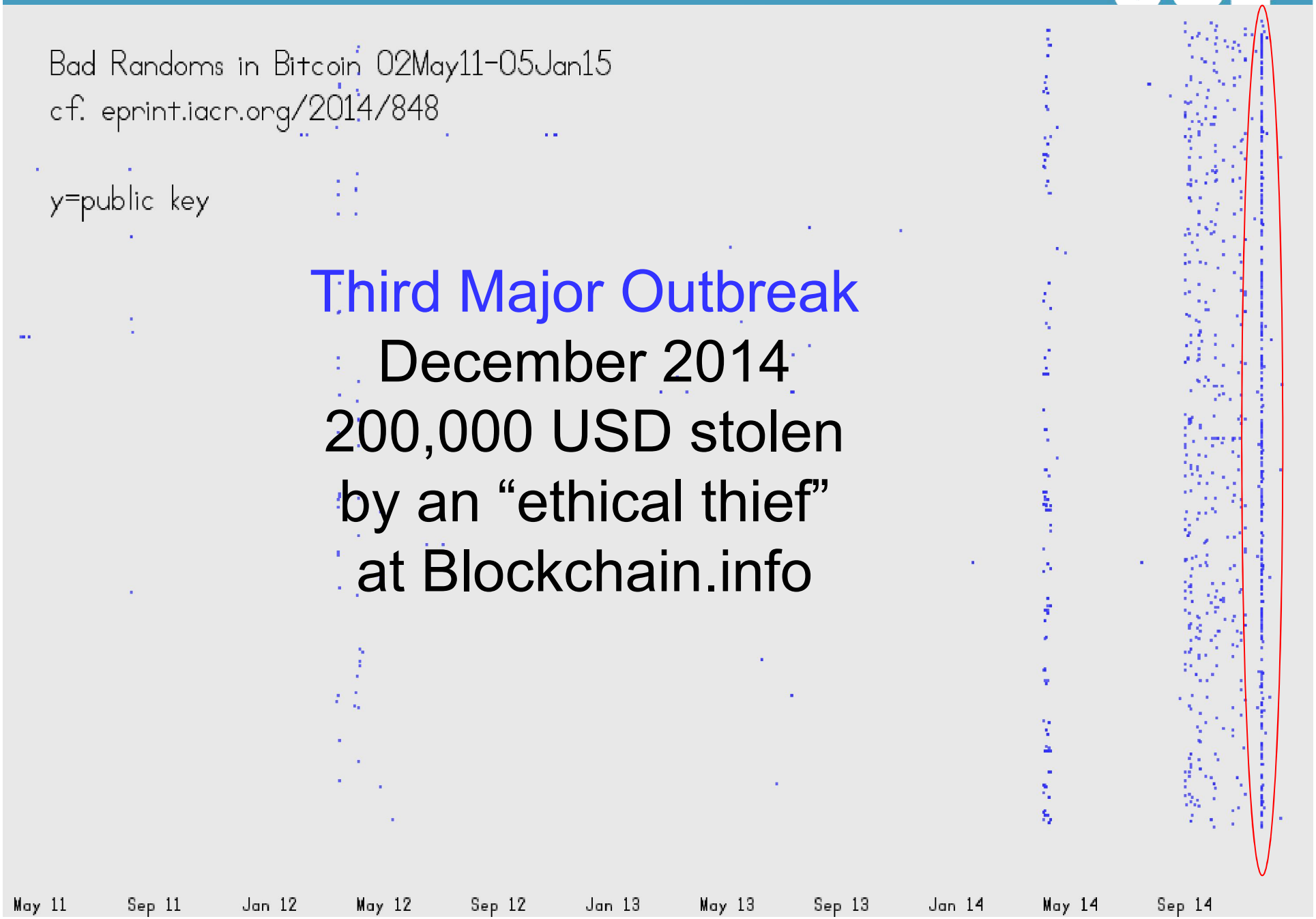
The money from the thefts is stored at:

https://blockchain.info/address/1HKywxiL4JziqXrzLKhmB6a74ma6kxbSDj

Still sitting there, he is NOT trying to spend it…
too famous? Afraid to be traced and caught?

Second Major Outbreak – May 2014




Bad Randoms in Bitcoin 02May11-05Jan15
cf. eprint.iacr.org/2014/848
y=public key
Third Major Outbreak
December 2014
200,000 USD stolen
by an “ethical thief”
at Blockchain.info
May 11
Sep 11
Jan 12
May 12
Sep 12
Jan 13
May 13
Sep 13
Jan 14
May 14
Sep 14

Dodgy Security Advice By A Thief

'Good Samaritan' Blockchain Hacker Who Returned 267 BTC Speaks Out

Jon Southurst (@southtopia) | Published on December 12, 2014 at 14:41 GMT

"johoe recommends a client that employs
HD (hierarchical deterministic) wallets,
such as Bread Wallet on iOS and Armory, Electrum or Wallet32 on Android."

Dodgy Security Advice By A Thief

'Good Samaritan' Blockchain Hacker Who Returned 267 BTC Speaks Out

Jon Southurst (@southtopia) | Published on December 12, 2014 at 14:41 GMT

"johoe recommends a client that employs
HD (hierarchical deterministic) wallets,
such as Bread Wallet on iOS and Armory, Electrum or Wallet32 on Android."

Is he not aware that these solutions can lead to thefts at a much larger scale?

Dodgy Security Advice By A Thief

CoinDesk

'Good Samaritan' Blockchain Hacker Who Returned 267 BTC Speaks Out

Jon Southurst (@southtopia) | Published on December 12, 2014 at 14:41 GMT

"johoe recommends a client that employs
HD (hierarchical deterministic) wallets,
such as Bread Wallet on iOS and Armory, Electrum or Wallet32 on Android."

Is he not aware that these solutions can lead to thefts at a much larger scale?

=> see our paper 2014/848.

Most Recent Bad Randoms

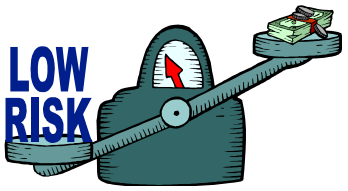
From my own scan:

c471b1ce535f6331d07759eeaafab4c1a276cdafa86245a7bf61f
29236619367

Appears 7 times in block 337458

4 January 2015

Used by different users…



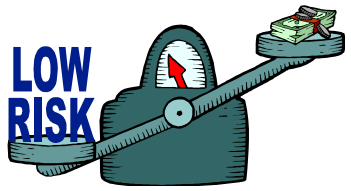
New Risks

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 were affected until today



Advanced Attacks
October 2014

eprint/2014/848

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.

UCL

New Paper:

cf.

eprint.iacr.org/
2014/848/

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

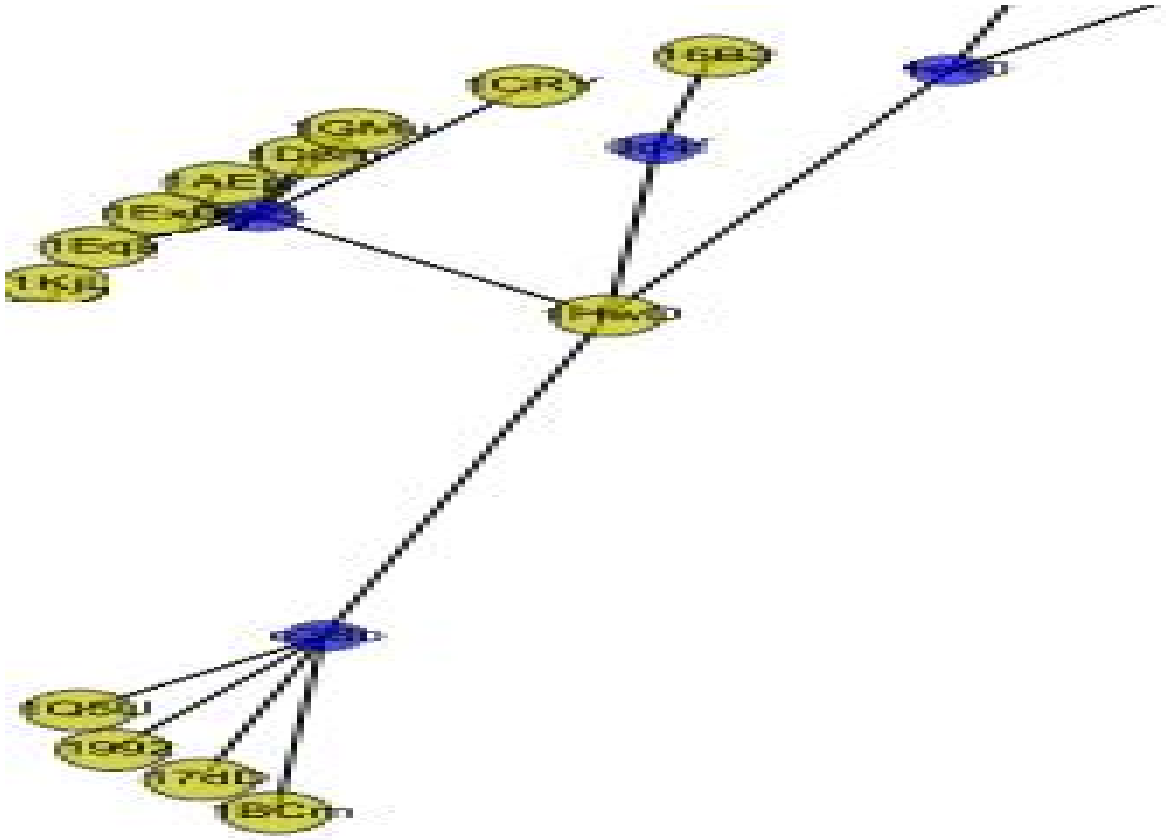
Nicolas T. Courtois[1] Pinar Emirdag[2] Filippo Valsorda[3]

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

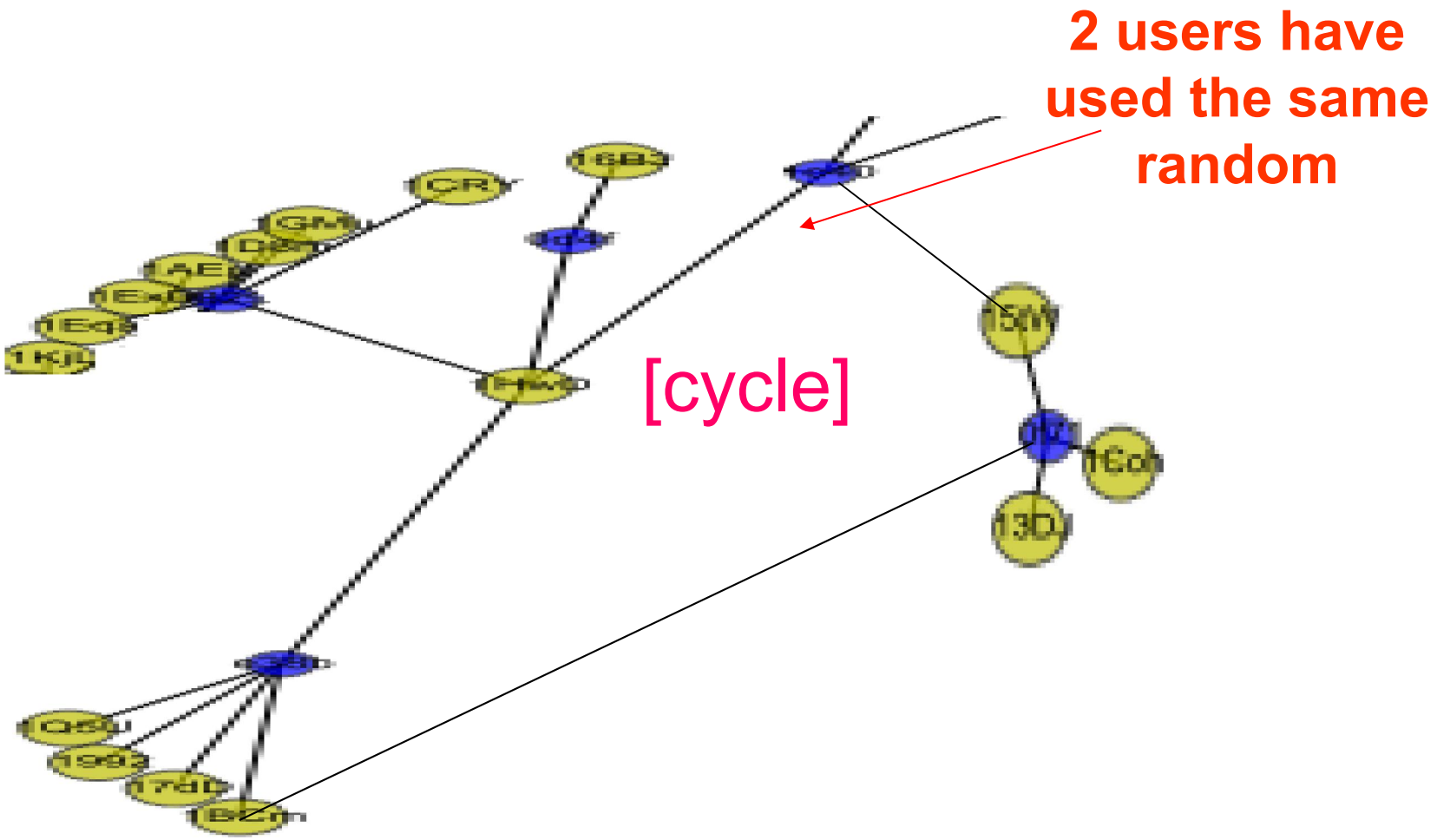
Abstract. In this paper we study the question of key management and practical operational security in bitcoin digital currency storage systems. We study the security two most used bitcoin HD Wallet key management solutions (e.g. in BIP032 and in earlier systems). These systems have extensive audit capabilities 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**.

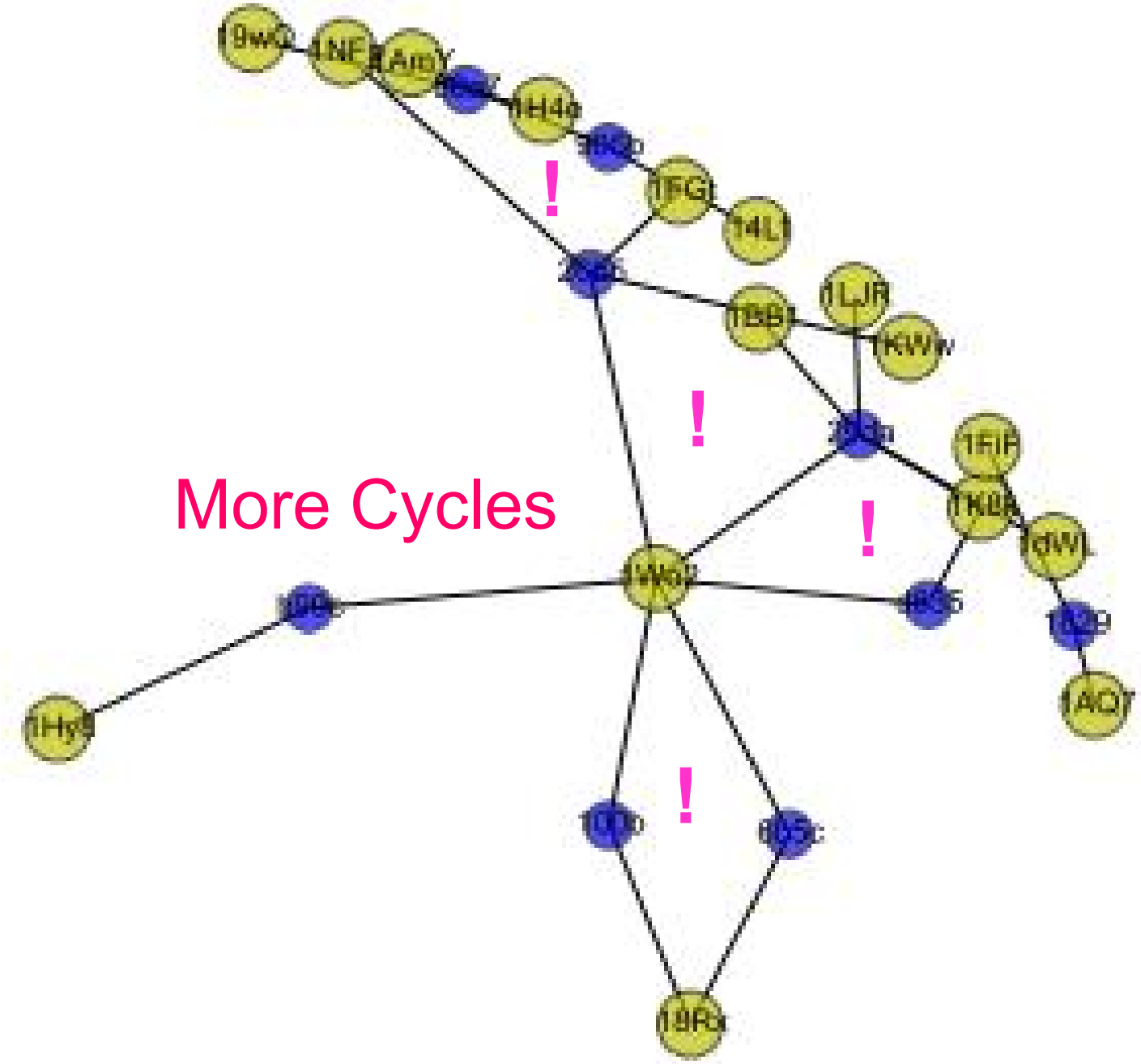
In our new attacks all bitcoins over whole large security domains can be stolen by people who have the auditor keys which are typically stored in hot systems connected to the Internet and can be stolen easily. Our combination attacks allow to recover private keys which none of the

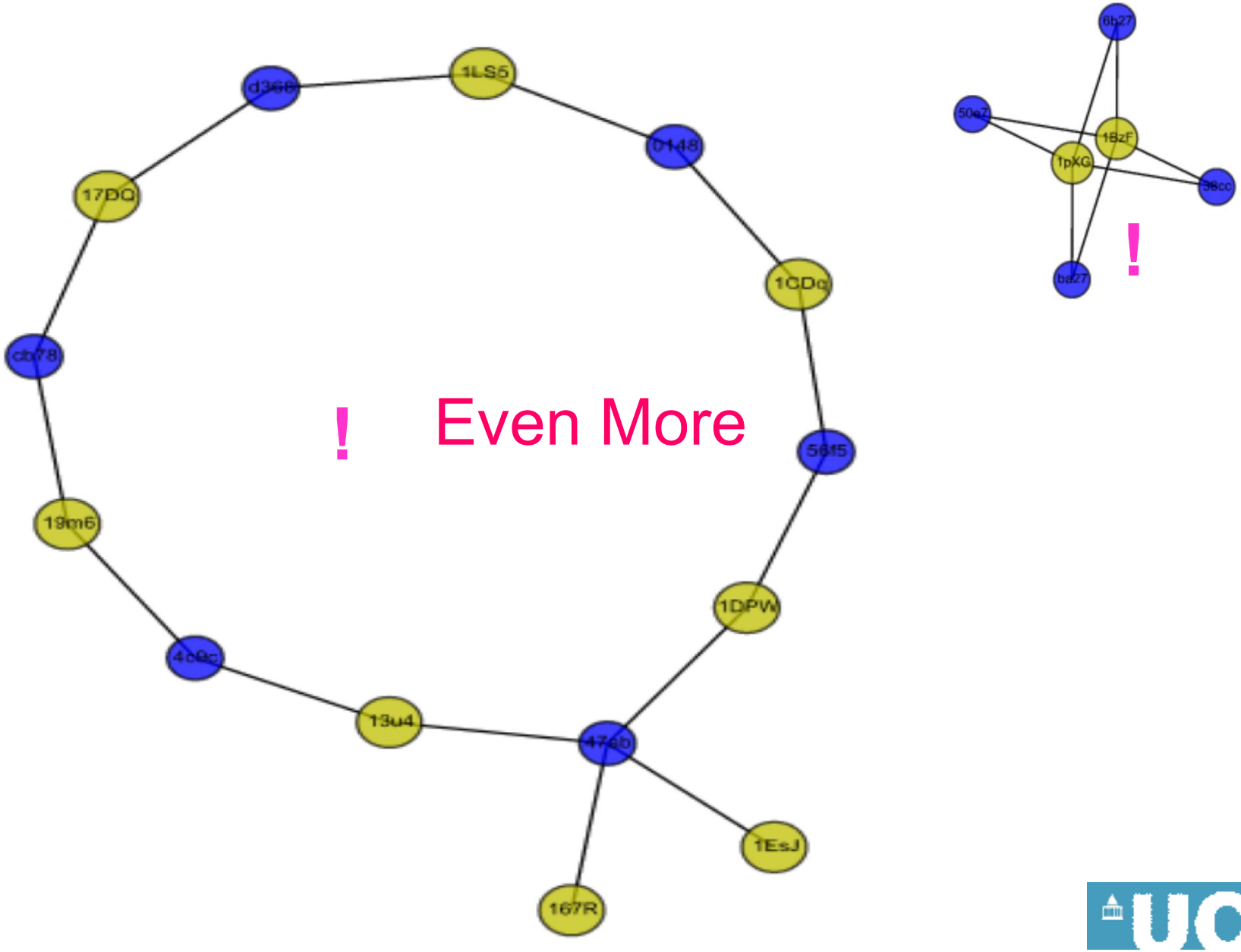
HD Wallets = Trees



2 Trees Connected Due to Bad Randoms




More Cycles
!
!
!
!


1LS5
d366
0148
17DQ
1CDq
cb78
! Even More
5615
19m6
1DPW
4c9q
13u4
476b
1EsJ
167R
6b27
50e7
1BzF
1pXG
36cc
bd27
!

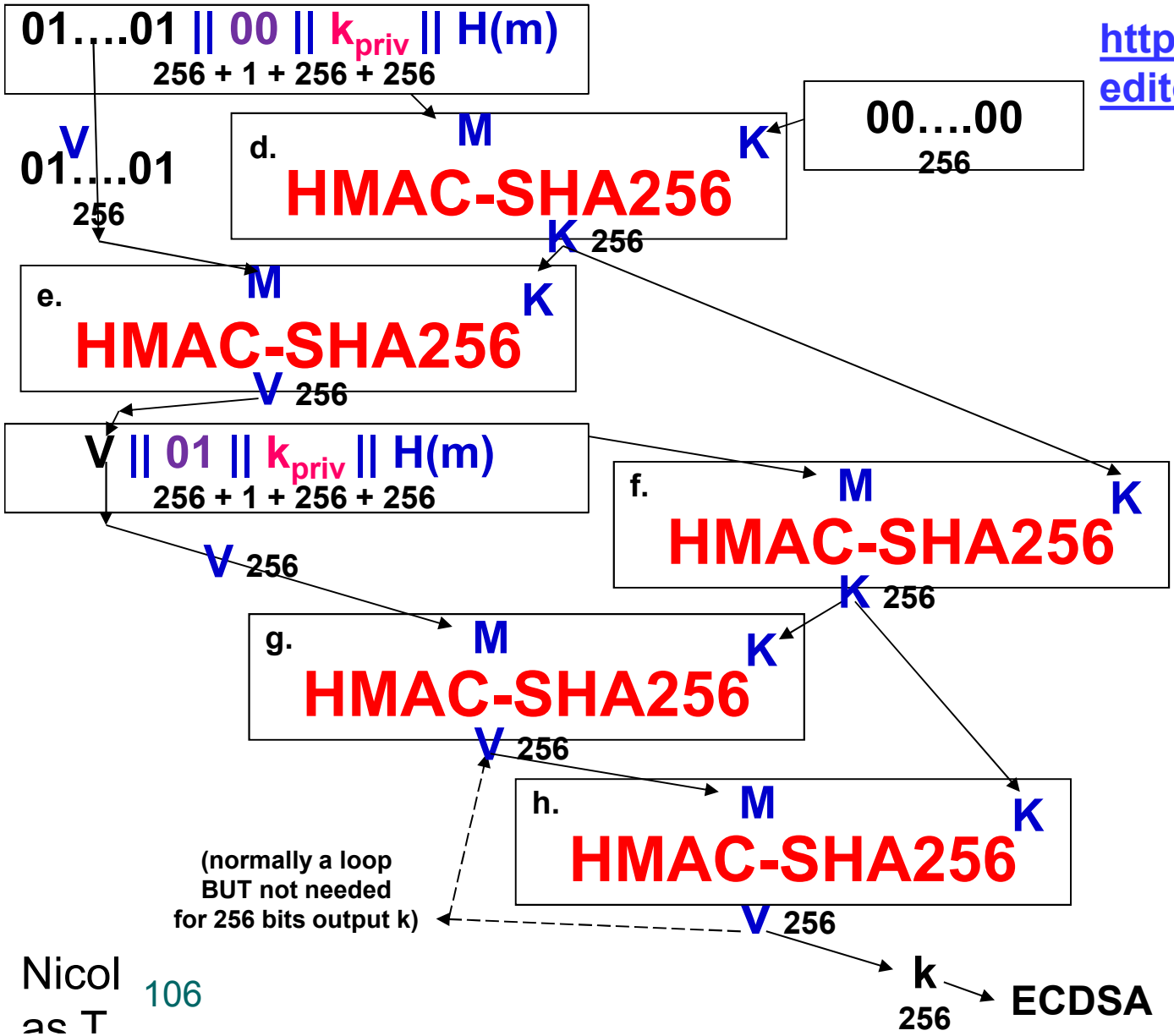
Is There a Fix?

Solution: RFC6979 [Thomas Pornin]

BOTTOM LINE:

If you have NOT implemented RFC6979,
you should be scared by this talk…

RFC6979 [Pornin] = 5+ applications of HMAC



http://www.rfc-editor.org/rfc/rfc6979.txt

Which Systems Are Affected?

Solution: RFC6979 [Pornin]

- Alredy applied by
  - Electrum,Multibit,Trezor
- Patched very lately:
  - blockchain.info – insecure,
  - Bitcoin Core – patch was applied 18M after being approved…