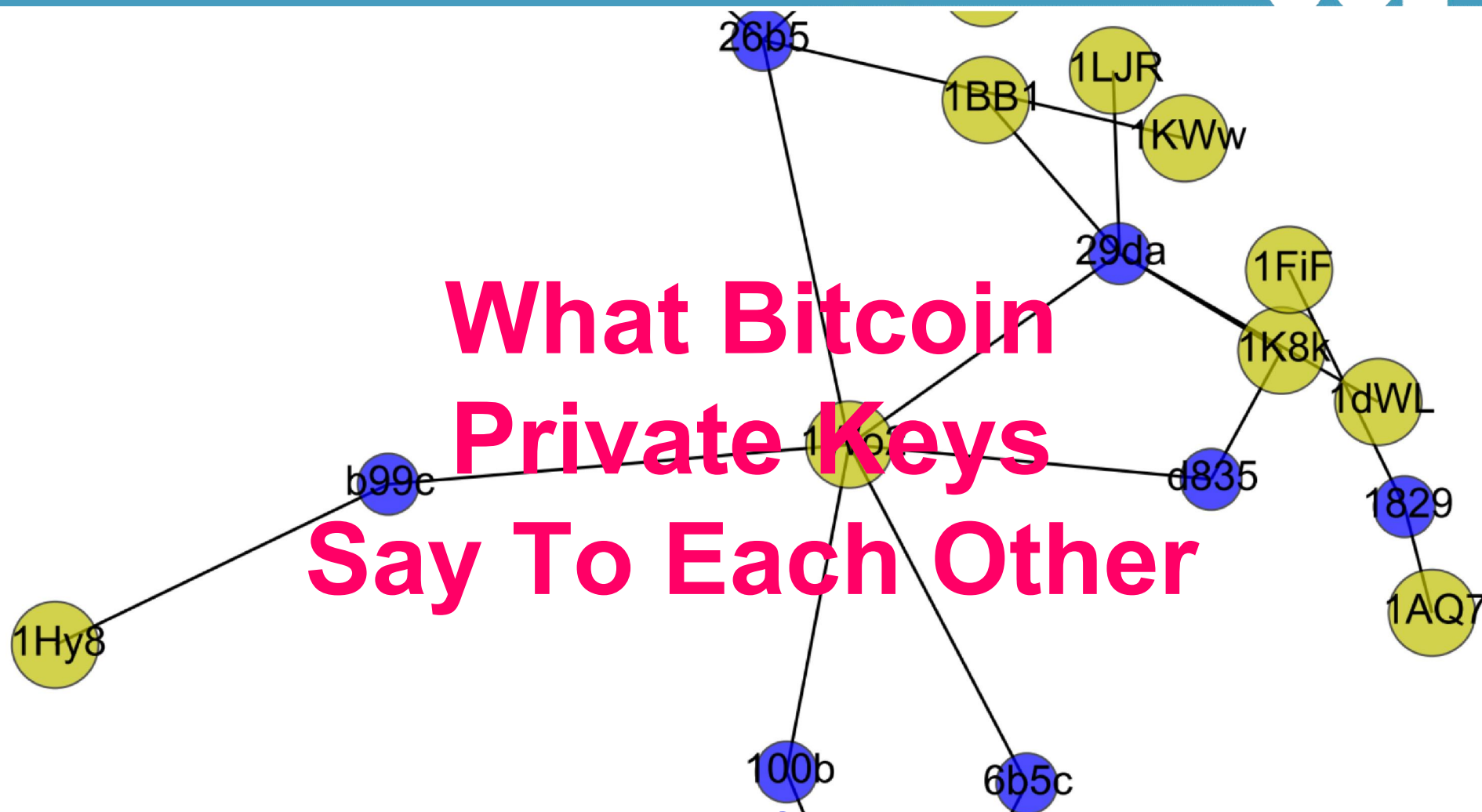


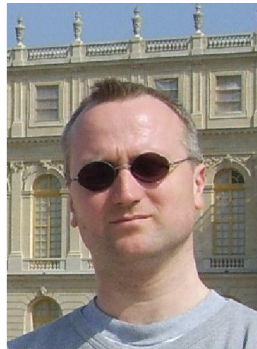
What Bitcoin Private Keys Say To Each Other



Nicolas T. Courtois

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

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)



 IACR Cryptographers





UCL Bitcoin Seminar

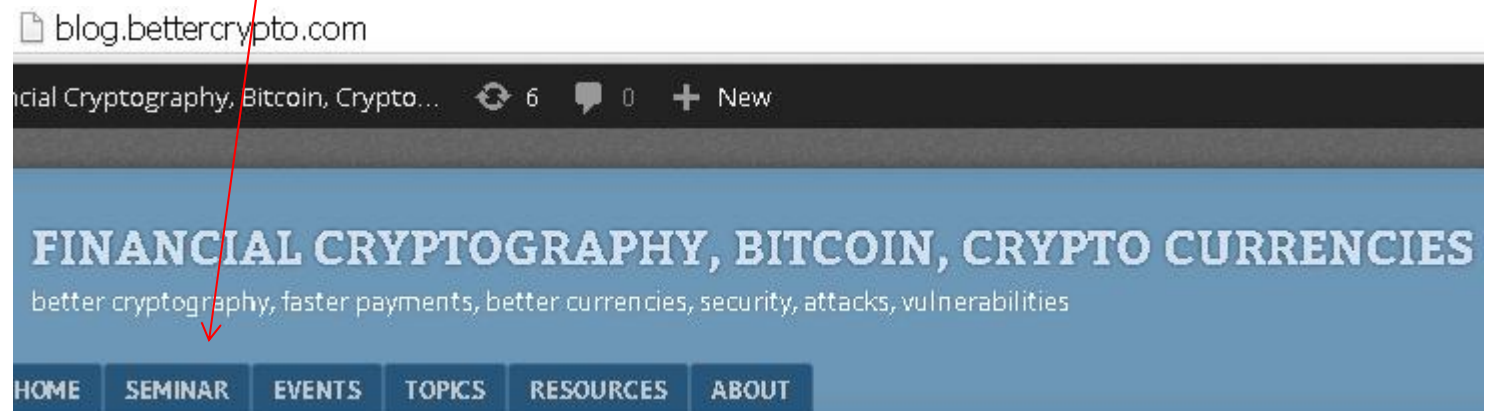
research seminar

=>In central London, runs EVERY WEEK!

public web page:

blog.bettercrypto.com / SEMINAR

or Google "UCL bitcoin seminar"



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.



Digital Currency

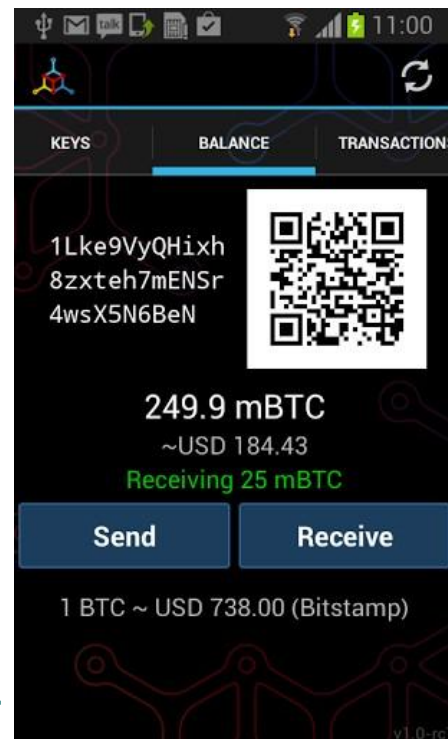
Bitcoin is a

=>PK-based Currency:

- bank account = a pair of public/private ECDSA keys
- spend money = produce a digital signature

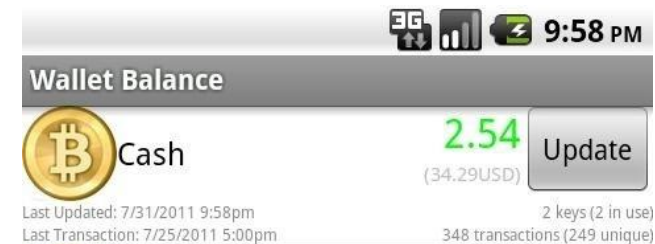


Wallets



Wallets

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



Block Chain

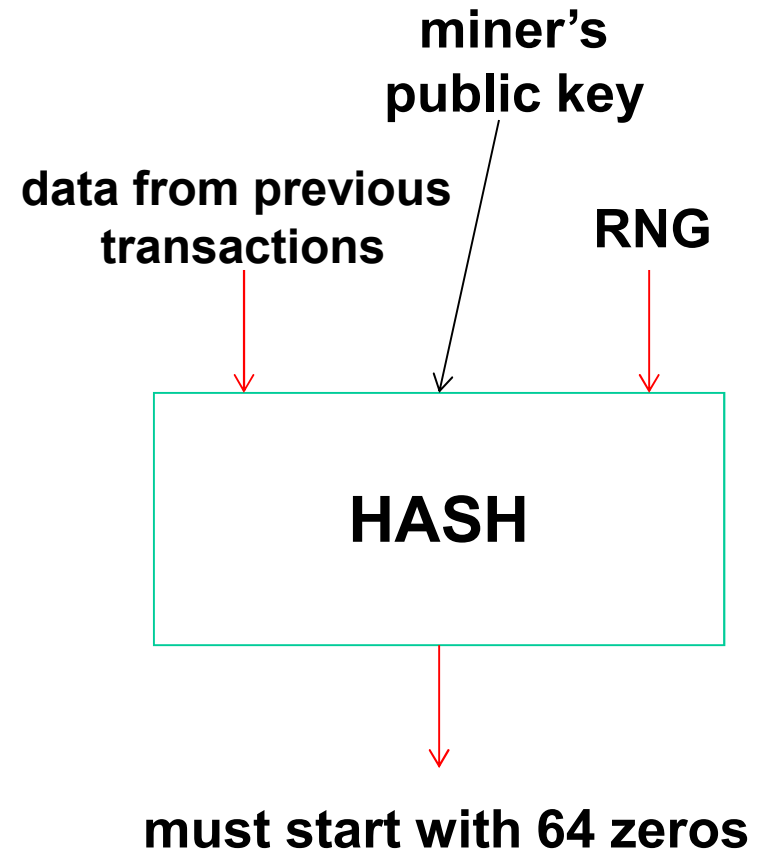


Bitcoin Mining

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

Ownership:

- “policed by majority of miners”:



Block Chain

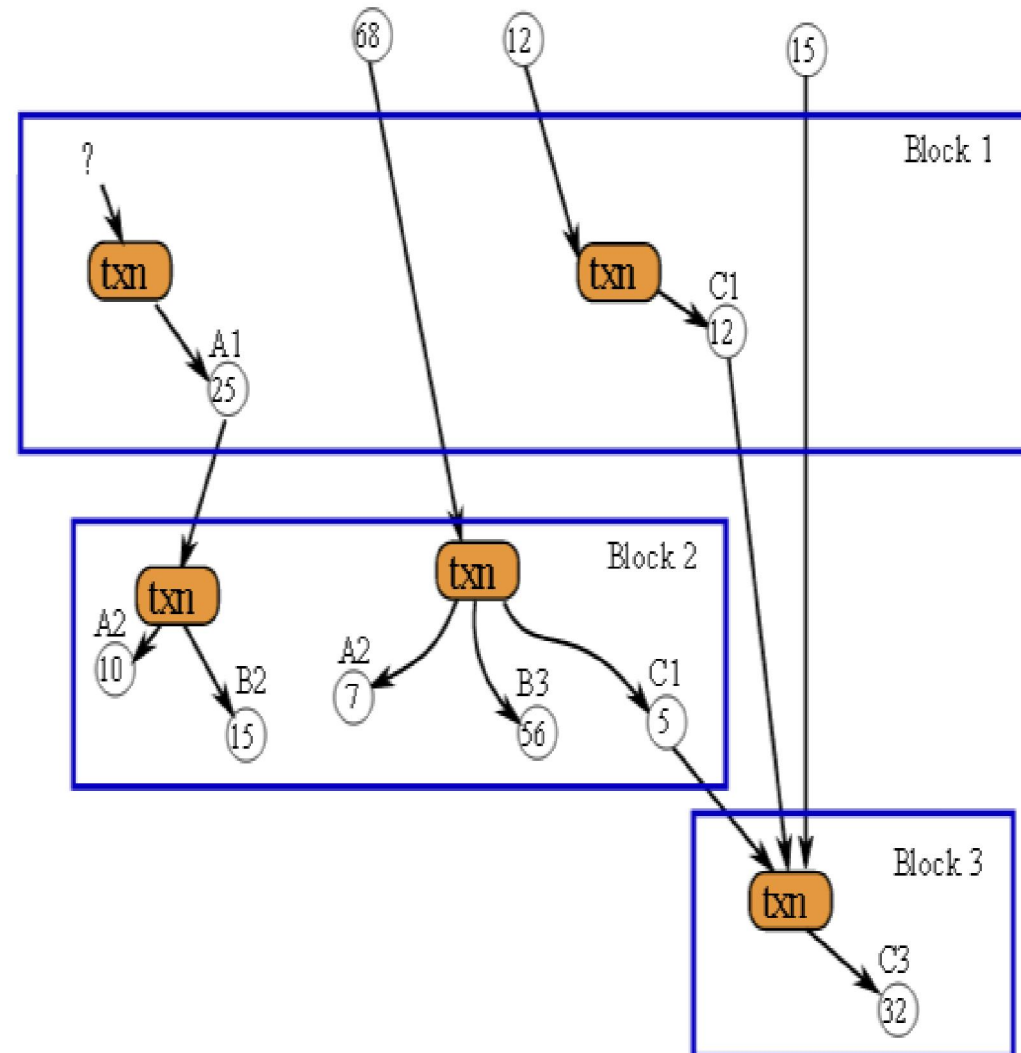
Def:



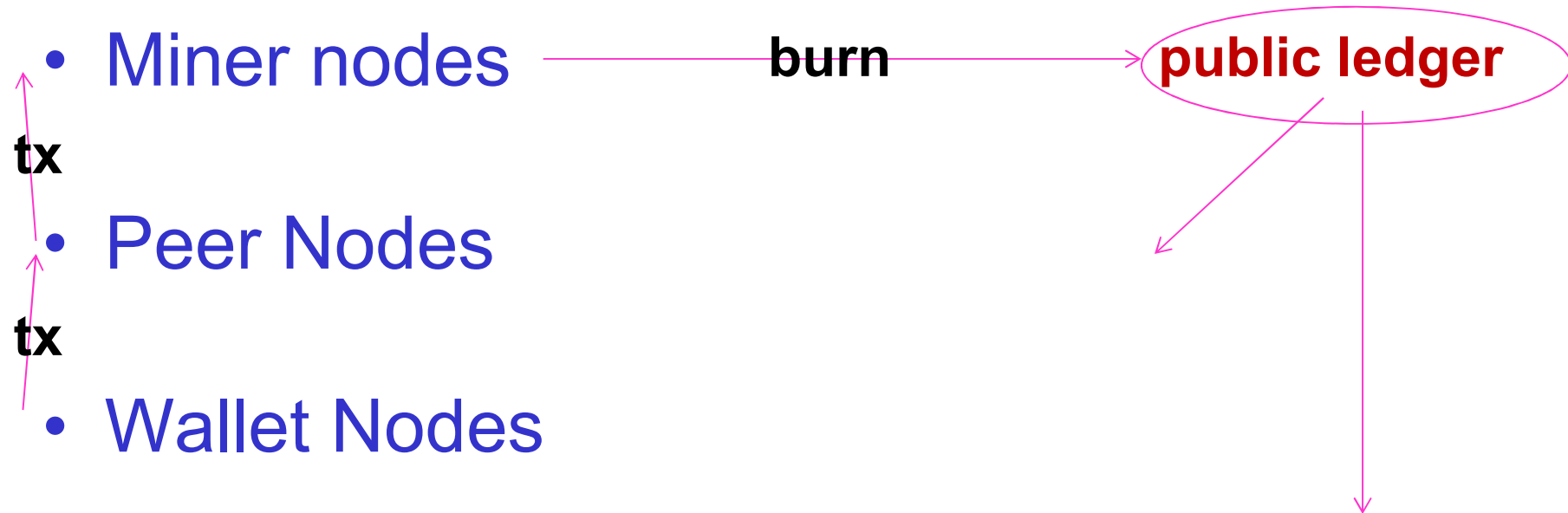
A transaction database
shared by everyone.

Also a ledger.

Every transaction
since ever is public.



Tx LifeCycle



Bitcoin Address

A screenshot of a Bitcoin transaction form. It has a light green background and a black border. The text "To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36" is on the first line, and "Amount: 1.0 BTC" is on the second line. A blue button with the word "SEND" in white capital letters is positioned at the bottom right of the form.

To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36
Amount: 1.0 BTC

Ledger-Based Currency

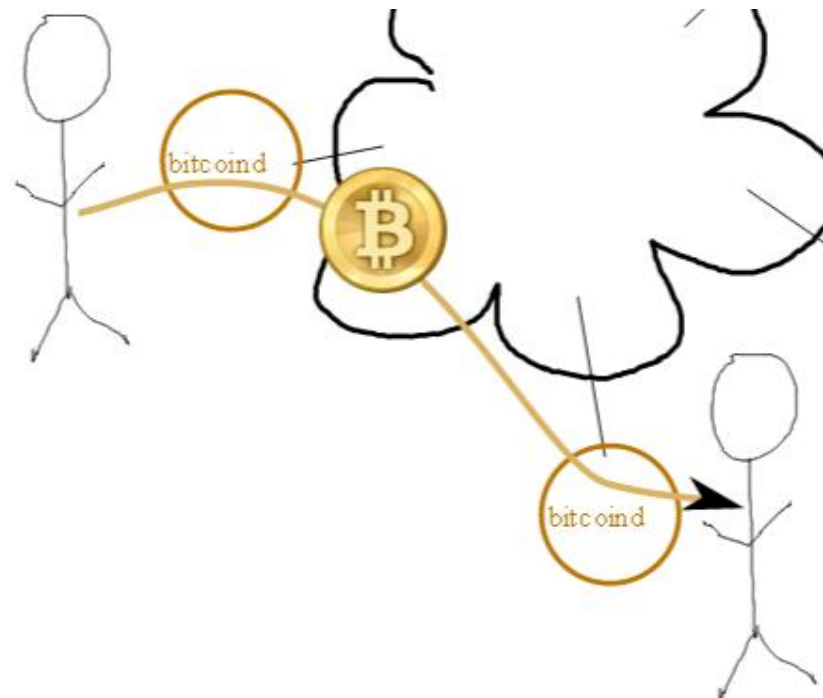
A “Bitcoin Address” = a sort of equivalent of a bank account.

Remarks:

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

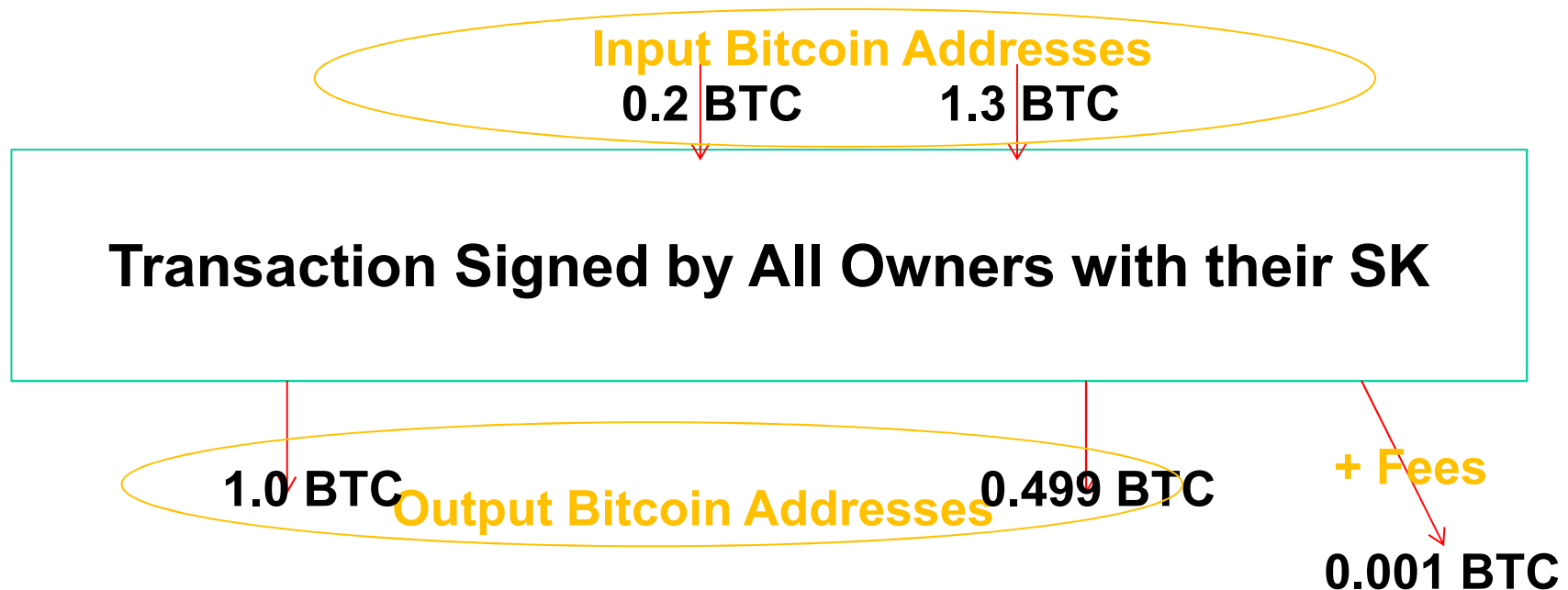
BTC Transfer

To: 1K2CcfWYW5sBL2xSeQWxpcmjPCgoXdi36
Amount: 1.0 BTC



Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



Transaction Scripts

Signed Tx

byte by byte

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)

Typical 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		
	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		
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		
	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		

scriptSig1
signature
(r,s)

scriptSig2
=Pkey
=(x,y)

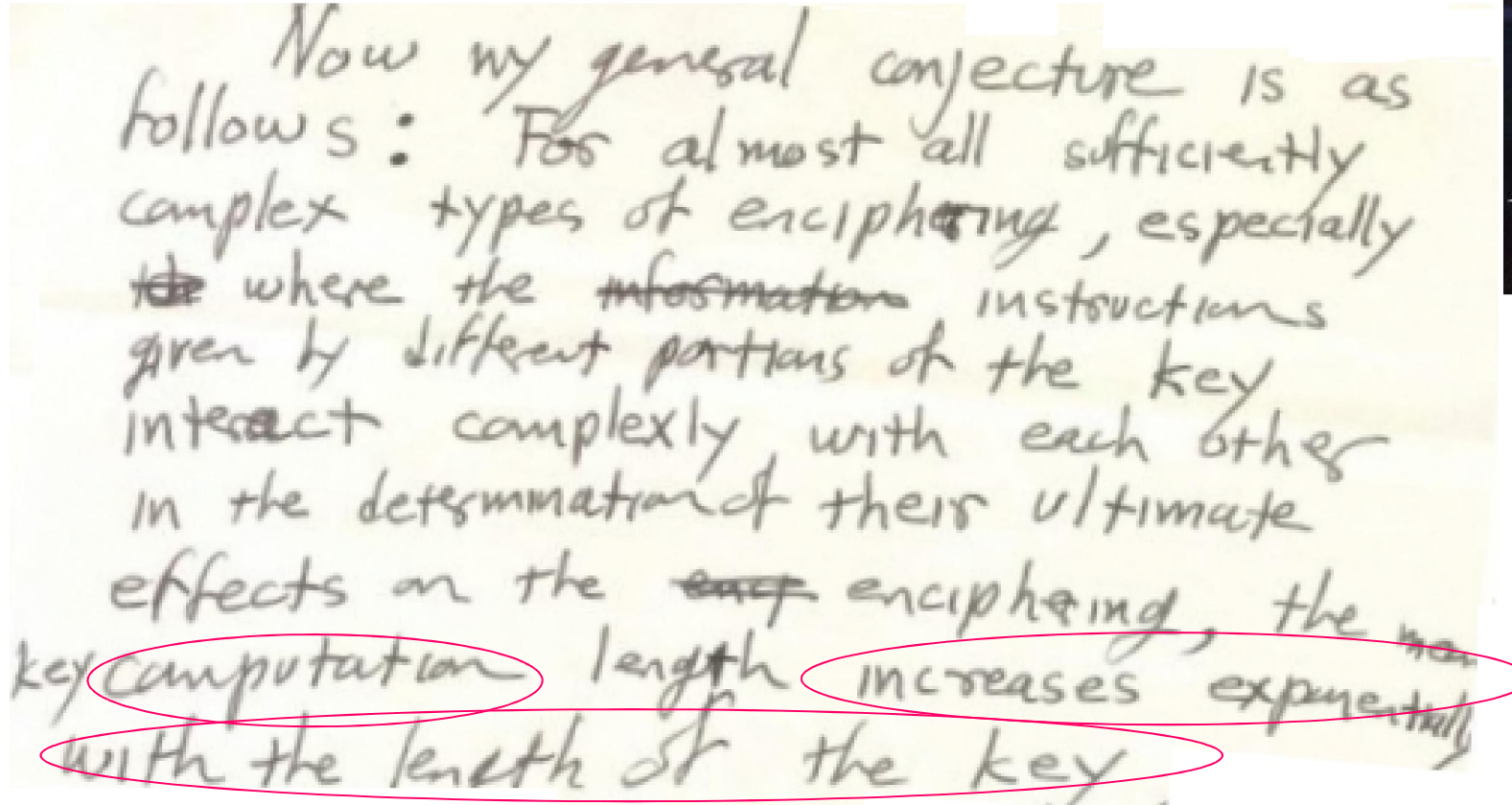
Is Bitcoin Secure?

Satoshi claimed it is...

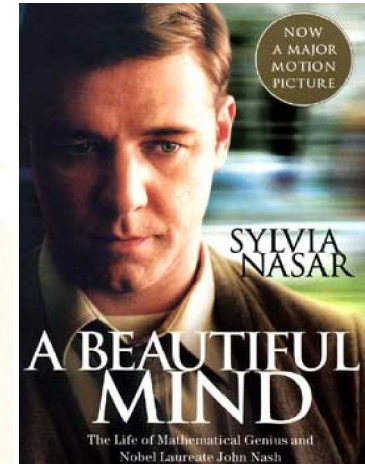


John Nash - 1955

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 ~~max~~ key computation length increases exponentially with the length of the key.

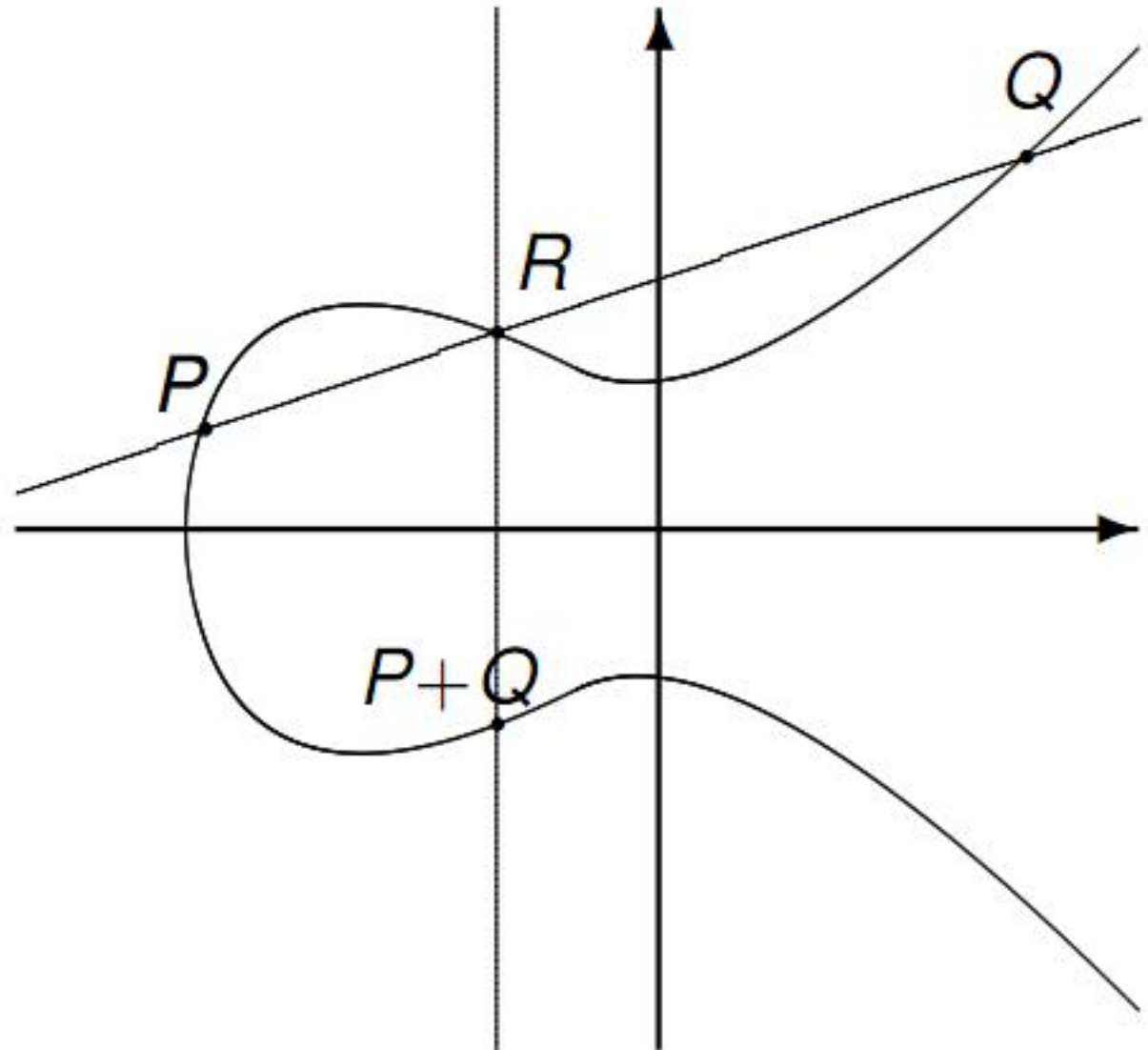
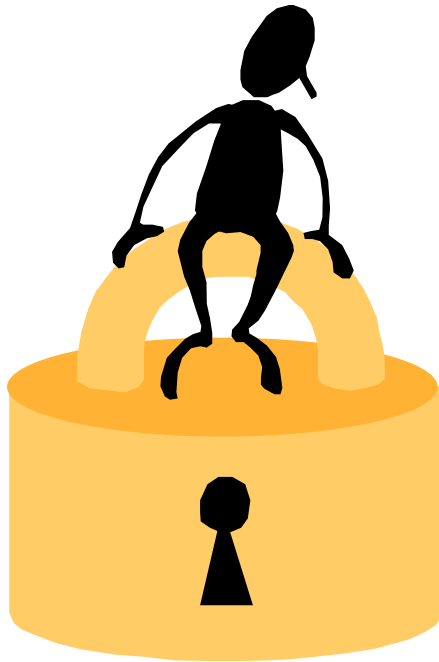


He also says that:

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

Elliptic Curve Crypto

“exponential
security”



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 \$**.

Official Bitcoin Wiki

[https://en.bitcoin.it/wiki/Myths# Bitcoins are worthless because they're based on unproven cryptography](https://en.bitcoin.it/wiki/Myths# Bitcoins_are_worthless_because_they're_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're based on unproven cryptography](https://en.bitcoin.it/wiki/Myths# Bitcoins_are_worthless_because_they're_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.

- ⇒ Not true!
 - ⇒ 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 ☺

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 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.

Crypto Challenges:

I always liked this idea.

Made cash bets on cryptography since 2001.

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

secp256k1
NOT INCLUDED
 no price if you
 break it ☹

TOTAL = 725,000 USD



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>

Bitcoin EC

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

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

*Special Multiples

Like “shortcuts in space”.

Fact: for the bitcoin elliptic curve
there exists SOME (not many)
special multiples
such that:

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

1000 of μ s in general
50 μ s for bitcoin curve

0.2 μ s general curve
0.05 μ s bitcoin curve

5363ad4cc05c30e0a5261c028812645a122e22ea20816678df02967c1b23bd73

7ae96a2b657c07106e64479eac3434e99cf0497512f58995c1396c28719501ef

Extremely Few Such Points

At <http://safecurves.cr.yp.to/disc.html> we read:

Such curves allow “slight speedups” for discrete log attacks however
“the literature does not indicate any mechanism that could allow further
speedups”.

So until now this problem is not considered as very serious...
However most cryptographers will tell you to avoid this curve.

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

What If? CataCrypt Conference

← → ↻ catacrypt.net/program.html



cataCRYPT



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)

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.



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

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

Incidents at Operation: Bad Randoms

German Army 1930s - Message Keys

(should be 3
random letters)

~~AAA~~

~~XYZ~~

~~ASD~~

QAY



Operators always found a way to «degrade » their
security

Old Stuff?

Not quite.

This is still happening
every day as we speak..

Modern Passwords

Main insight:

these mistakes do not die, they live forever,

=>absolutely EACH AND EVERY of these common mistakes or patterns is still present TODAY as a distinct patterns in real-life probability distributions on human-generated passwords.

Examples:

8.5% of people use 'password' or '123456'

91% of people use one of top 1000 passwords

[source: xato.net]

Brain Wallets

Maybe the only safe way to transport money for refugees in transit.



Brain Wallets

We have recovered private keys for some 18,000 bitcoin wallets.

Private key: SHA256("password")

5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8

See also presentation by Ryan Castellucci
@DefCon 23 (Aug 2015).

At UCL we have been mining these weak passwords since early 2015 after initial discoveries made by our students.

We have also improved Ryan's code.

Speed Optimizations in Bitcoin Key Recovery Attacks

Nicolas Courtois
University College London
n.courtois@ucl.ac.uk

Guangyan Song
University College London
g.song@cs.ucl.ac.uk

Ryan Castellucci
White Ops
pubs@ryanc.org

Our Paper

ABSTRACT

In this paper we study and give the first detailed benchmarks on existing implementations of the secp256k1 elliptic curve used by at least hundreds of thousands of users in Bitcoin and other cryptocurrencies. Our implementation improves the state of the art by a factor of 2.5, with focus on the cases where side channel attacks are not a concern and a large quantity of RAM is available. As a result, we are able to scan the Bitcoin blockchain for weak keys faster than any previous implementation. We also give some examples of passwords which we have cracked, showing that brain wallets are not secure in practice even for quite complex passwords.

Keywords

Bitcoin, Elliptic Curve Cryptography, Crypto Currency, Brain Wallet

Everyone on the network can verify the signature that has been sent out. Anyone can spend all the bitcoin in a bitcoin address as long as they hold the cosponsoring private key. Once the private is lost, the bitcoin network will not recognize any other evidence of ownership.

Bitcoin uses digital signature protect the ownership bitcoin and private key is the only evidence of owning bitcoin. Thus it is very important to look at the technical details of the digital signature scheme used in bitcoin.

1.1 Structure of the paper

In this paper we study and give the first detailed benchmarks on existing secp256k1 elliptic curve implementations used in Bitcoin. Section 2 introduces background knowledge about elliptic curve cryptography and brain wallets. Section 3 reviews previous research work in this area. Section 4 gives detailed benchmark for existing method and our own implementation. Our implementation improves the state of the

Some Results

“say hello to my little friend”

“to be or not to be”

“Live as if you were to die tomorrow.
Learn as if you were to live forever.”

“This is the way the world ends.”

More Passwords

- “andreas antonopoulos”
- “mychemicalromance9”
- “yohohoandabottleofrum”
- “dudewheresmycar”
- “youaremysunshinemyonlysunshine”
- “THIS IS IT”
- “Arnold Schwarzenegger”
- “these aren't the droids you're looking for”
- “nothing ventured nothing gained”
- ...

Speed

Table 7.5: Time cost for different window width w for EC key generation

	w=4	w=8	w=12	w=16	w=20
d	64	32	22	16	13
number of additions	63	31	21	15	12
precomputation memory	81.92 KB	655.36 KB	7.21 MB	83.89 MB	1.09 GB
secp256k1_gej_add_ge	45.85 us	22.16 us	15.35 us	11.23 us	9.23 us
secp256k1_gej_add_ge_var	37.37 us*	17.86 us	12.21 us	8.89 us	7.16 us
7M + 4S code	39.01 us	18.79 us	12.77 us	9.23 us	7.48 us
covert Jacobian to Affine	≈ 10 us				
Defcon Attack i7-2600 3.2 GHz CPU	≈ 130 K guesses / sec				
Our implementation i7-3520m 2.9 GHz CPU	≈ 375 K guesses / sec				

MiFare Classic

Nicolas T. Courtois: **The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime**, In SECRYPT 2009, pp. 331-338.

Nicolas Courtois, Daniel Hulme, Kumail Hussain, Jerzy Gawinecki, Marek Grajek: **On Bad Randomness and Cloning of Contactless Payment and Building Smart Cards**, In IWCC 2013, International Workshop on Cyber Crime, IEEE, San Francisco, May 2013, pp. 105-110.

<http://www.ieee-security.org/TC/SPW2013/papers/data/5017a105.pdf>



Best Attack on MiFare Classic?

- Use 'Courtois Dark Side' attack for one sector.
 - Google for MFCUK software
 - There are also links on blog.bettercrypto.com

Data Complexity

Use 'Courtois Dark Side' attack:

300 queries on average.

in comparison 3rd Nijmegen Oakland attack requires:

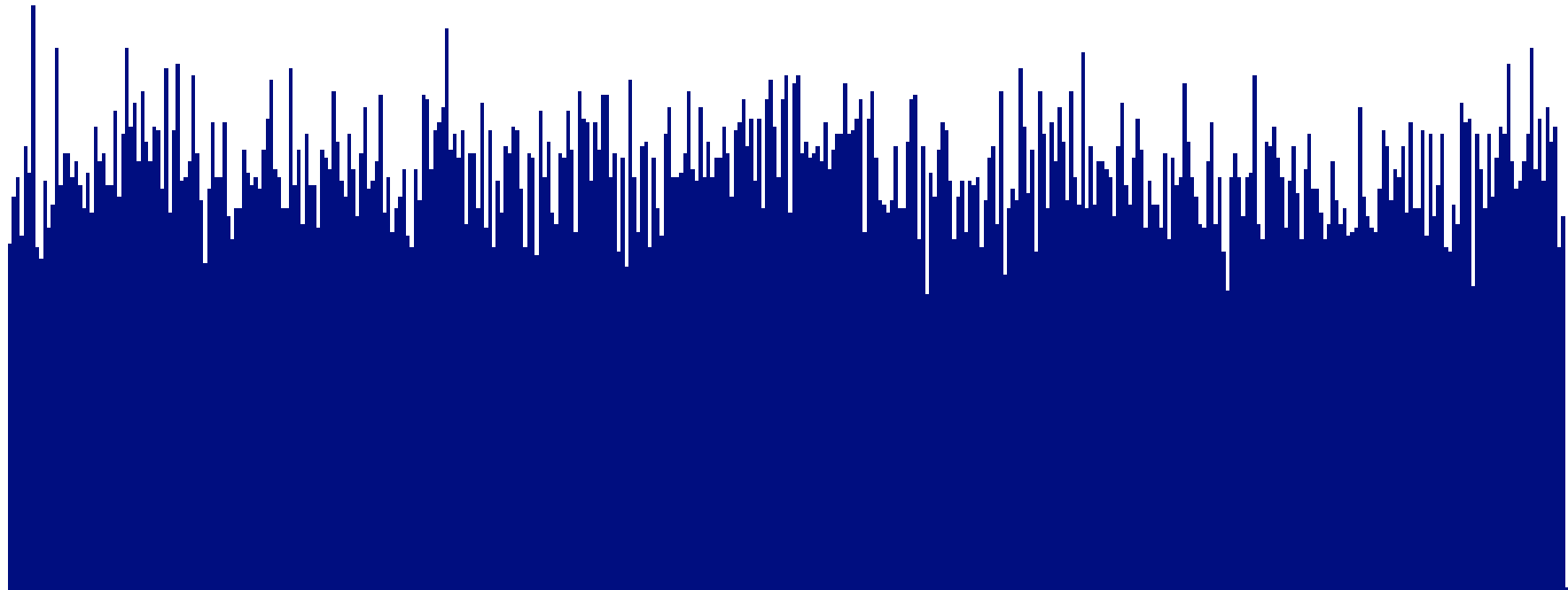
- pre-computed 384 Gbytes of data (EXPENSIVE)
- 4000 queries... (done in 2 minutes).

In Theory

The 'Courtois Dark Side' attack should crack smart cards in **10 SECONDS TOTAL** time.

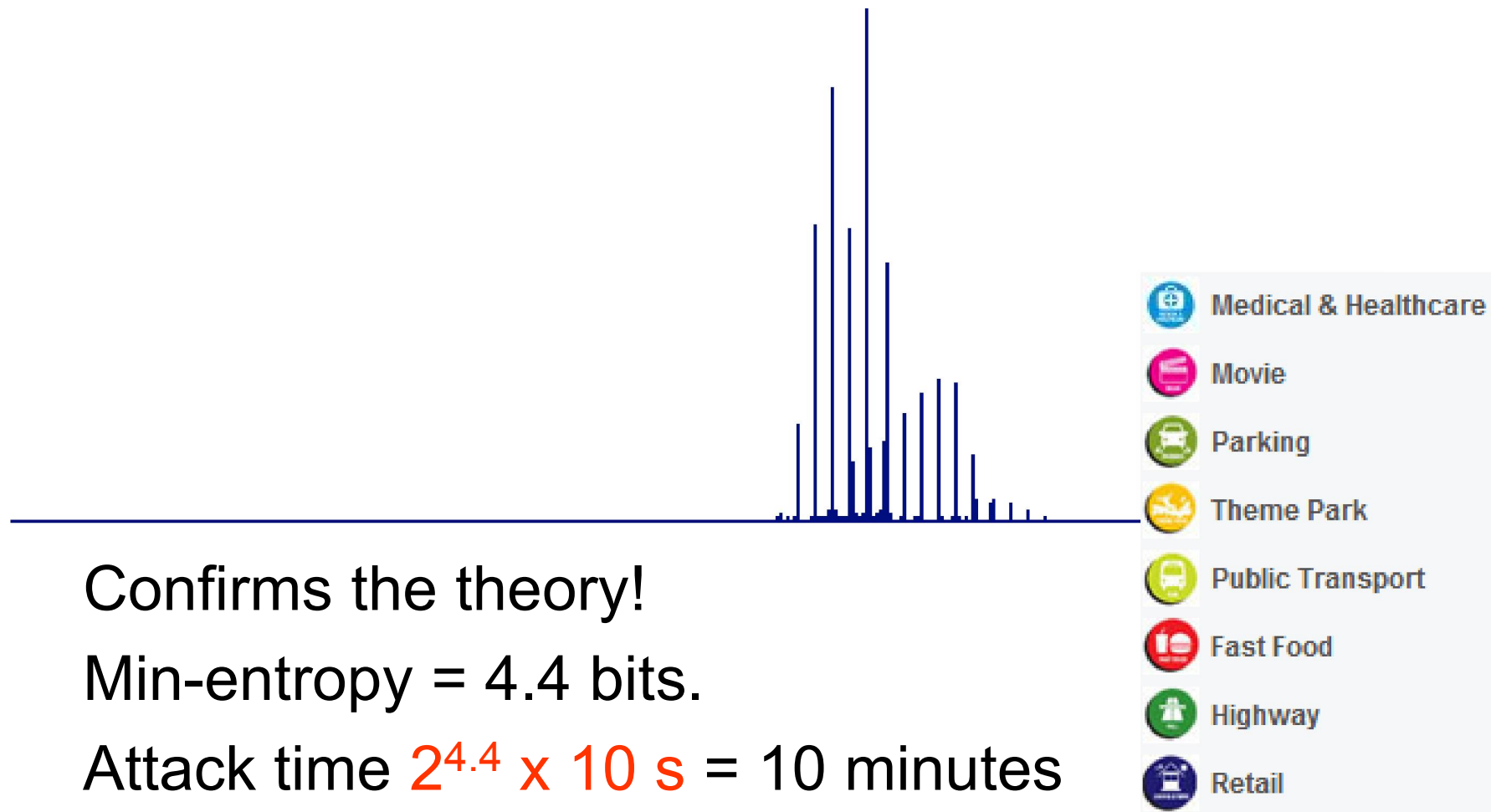
In practice it doesn't....

Experiment 1 – London University Card



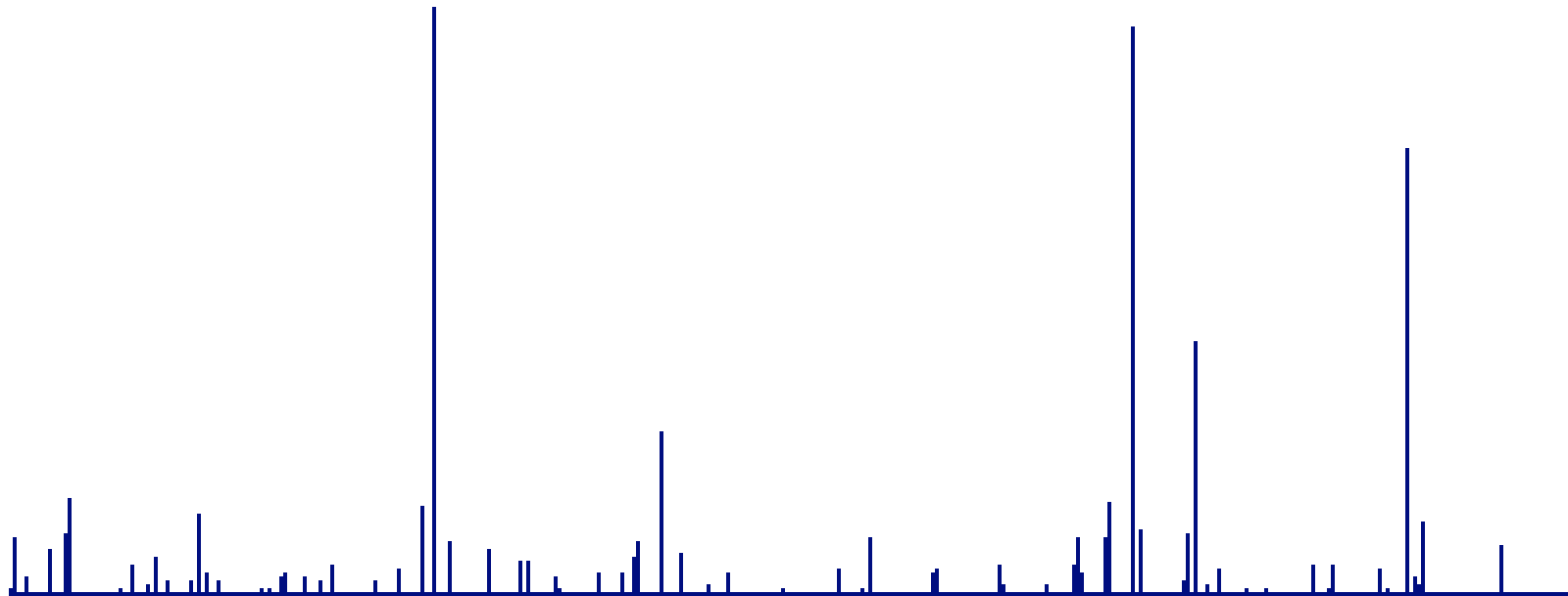
- Min-entropy = def=
 $\log_2(\text{most likely card random}) = 12.4 \text{ bits}$
 \Rightarrow Attack takes very roughly $2^{12.4} \times 10 \text{ s} = 1 \text{ day/key}$.

Experiment 2 – Malaysia Payment Card



- Confirms the theory!
- Min-entropy = 4.4 bits.
- Attack time $2^{4.4} \times 10 \text{ s} = 10 \text{ minutes}$

London Oyster Card From 2006



- Min-entropy = 2.8 bits.
- Attack time $2^{2.8} \times 10^6 \text{ s} = 3 \text{ minutes}$
-

Bad Randoms in Bitcoin



Bad Randoms in Bitcoin

First publicized by Nils Schneider:

28 January 2013

D47CE4C025C35EC440BC81D99834A624875161A26BF56EF
7FDC0F5D52F843AD1

⇒ repeated countless times...

⇒ used twice by the SAME user!

⇒ and twice by another user..

⇒ etc..



ECDSA Signatures

Let d be a private key, integer $\text{mod } n = \text{ECC [sub-]group order}$.

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

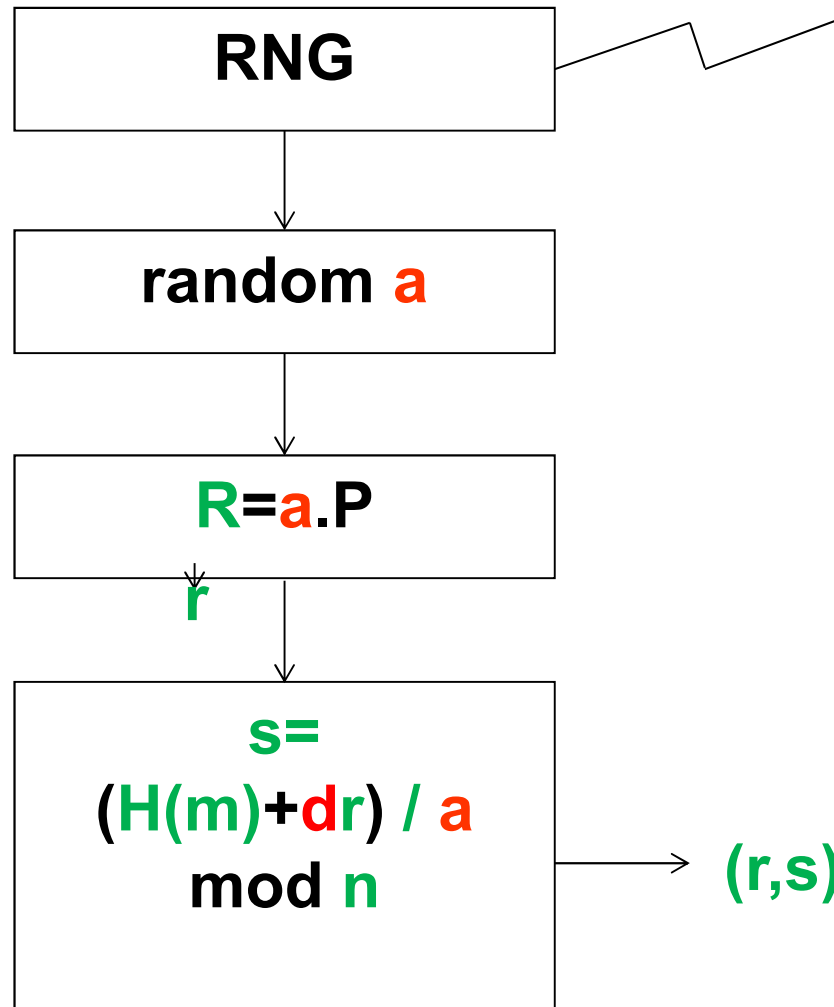
The signature of m is the pair (r, s) .

(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 =>

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

=>

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

each person can steal the
other person's bitcoins!

=>any of them CAN
recompute **k** used

Our Graph Model

8e9fafd24f498744078c375b42ea087f5c43c8a5131949d1e19df32e0b4f9a67

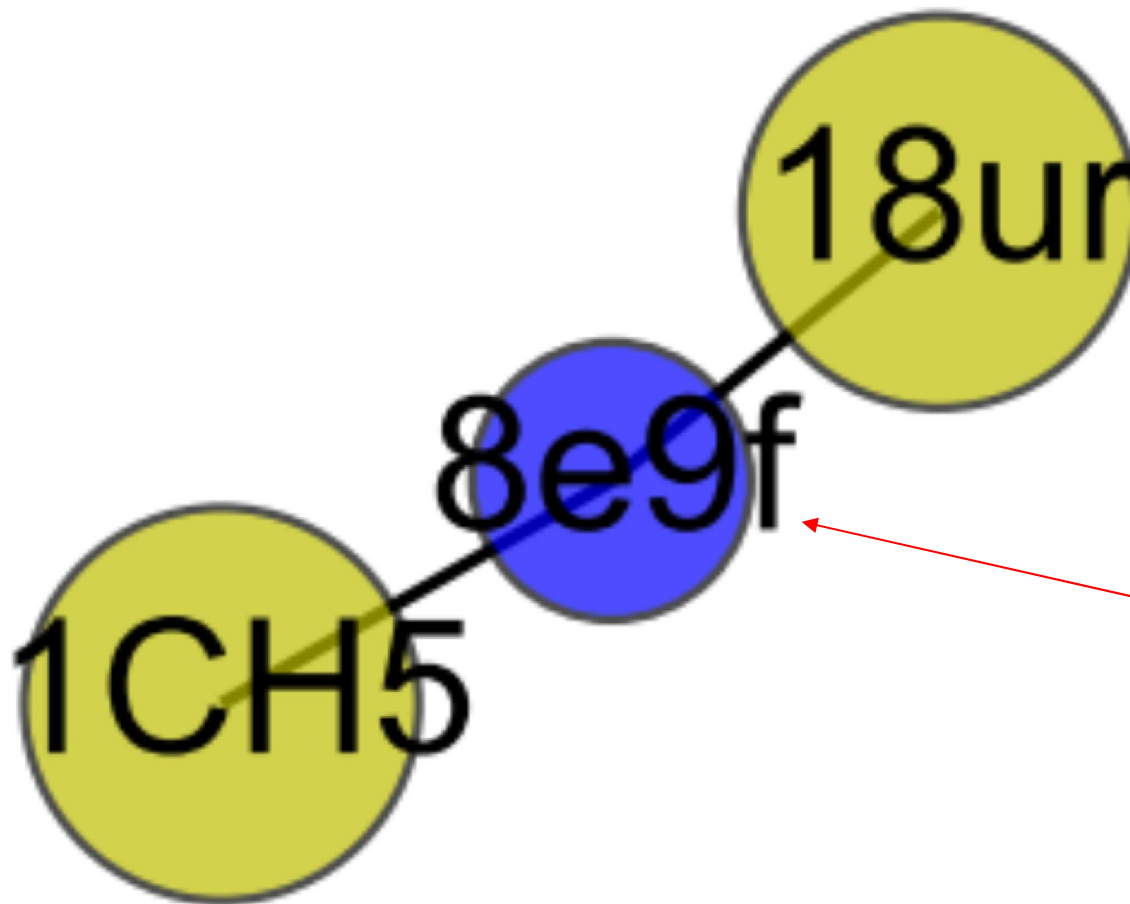
2x 09Jan15-09Jan15

1x [/1CH5R3DpWBgdbanOpHbJ8mtWCCWjHCx5ph](#)

[338168/tx533/i0](#)

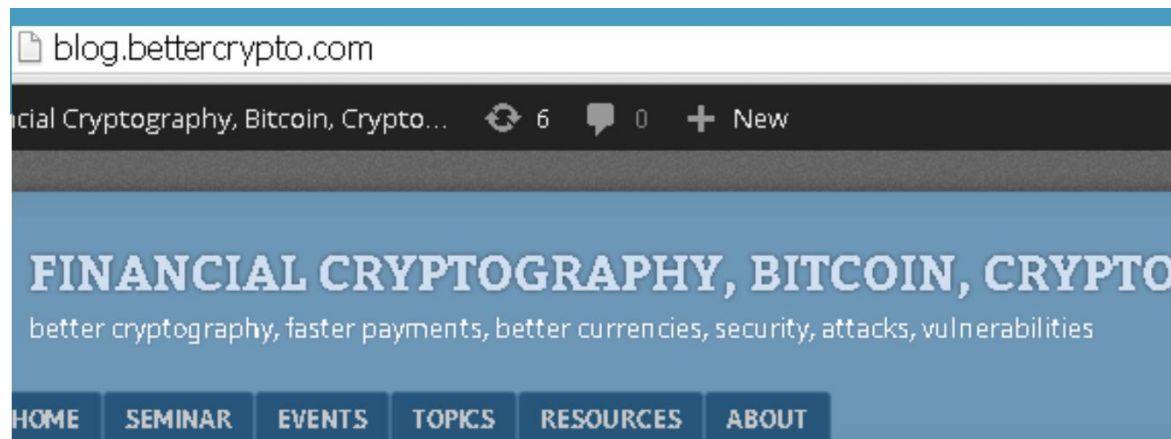
1x [/18urmgKfTMC8AihEUzj7CpZfsxmg5ZUovE](#)

[338168/tx533/i1](#)



**2 users have
used the same
random**

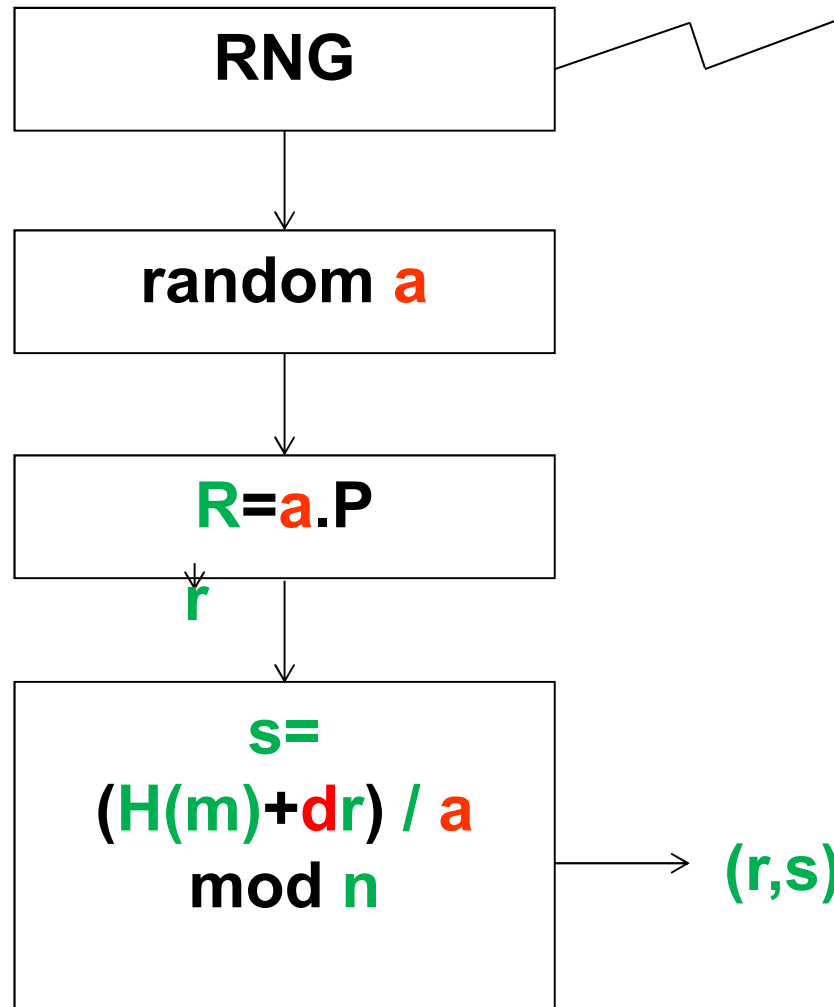
Our Online Database



9e199edb08bec948740e84cc6f91f0bbbf36bc5f10546e0c1a6e2655f2c6019	4x	07Jan15-07Jan15
1x / 1LR63Z94Lz29XVvnwaWi4JViREpFk4BFZf		337956/tx26/i3
1x / 12rdRMTZQ6uuVucRnPtSmZRoqp2MVgBmh9		337956/tx26/i1
1x / 1BPVuwza9pDHpbzUBMLUyhyV7PnuF2iJGx		337956/tx26/i2
1x / 147rzbsdsqc2YKeGQRUs3jaCxyufVRz8Kh		337956/tx26/i0
c471b1ce535f6331d07759eeaaafab4c1a276cdafa86245a7bf61f29236619367	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: $(s_1 a - H(m_1)) =$
rd =
 $(s_2 a - H(m_2)) \text{ mod } n$
 $\Rightarrow a = (H(m_1) - H(m_2)) / (s_1 - s_2)$
 $\text{mod } n$ AND now
 $d = (sa - H(m)) / r \text{ mod } n$

anybody can steal
the bitcoins!

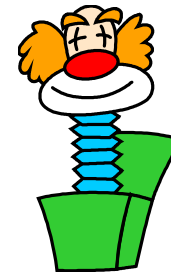
Have These Problems Stopped in 2013?

Lots of problems in May 2012, fixed.

2013: Android bug was fixed...

And then there was another MASSIVE outbreak...

And then another...



Dec. 2013

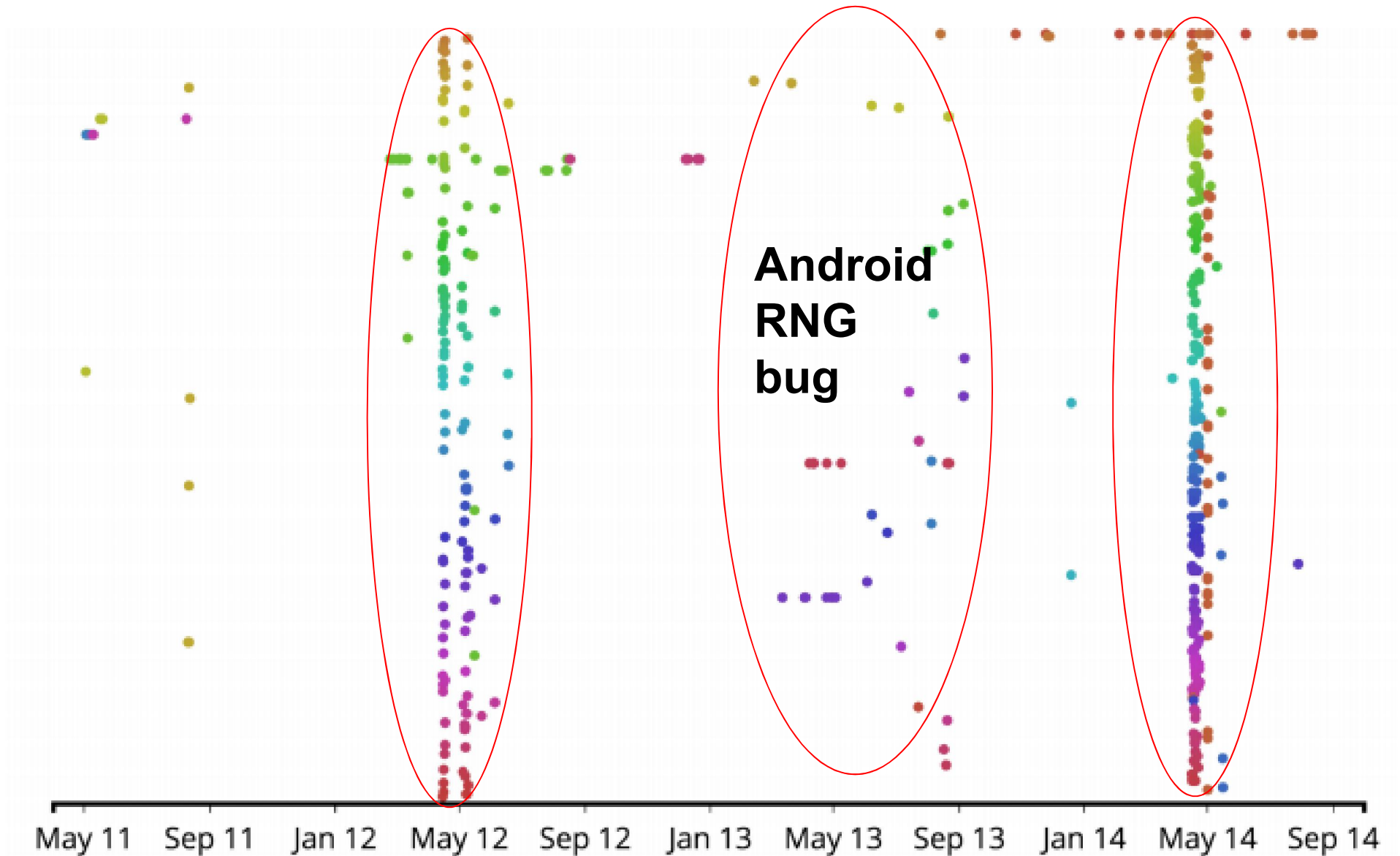
At 30C3 conference in Germany on 28 Dec 2013
Nadia Heninger have reported that they have identified
a bitcoin user on the blockchain
which has stolen some 59 BTC due to
these bad randomness events,

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

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



'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](#).

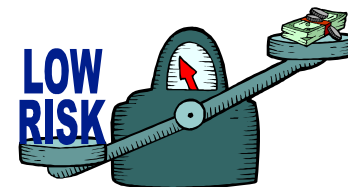
Most Recent Bad Randoms

From my own scan:

c471b1ce535f6331d07759eeaafab4c1a276cdafa86245a7bf61f
29236619367

Appears 7 times in block 337458
4 January 2015

Used by different users...



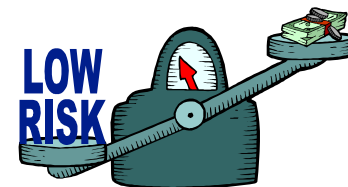
New Risks



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

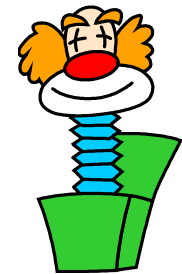
New attacks [Courtois et al. October 2014]

=> under certain conditons

ALL bitcoins in cold storage

can be stolen

=> millions of accounts potentially affected.





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

cf.

[eprint.iacr.org/
2014/848/](http://eprint.iacr.org/2014/848/)

Nicolas T. Courtois¹

Pinar Emirdag²

Filippo Valsorda³

¹ University College London, UK

² Independent market structure professional, London, UK

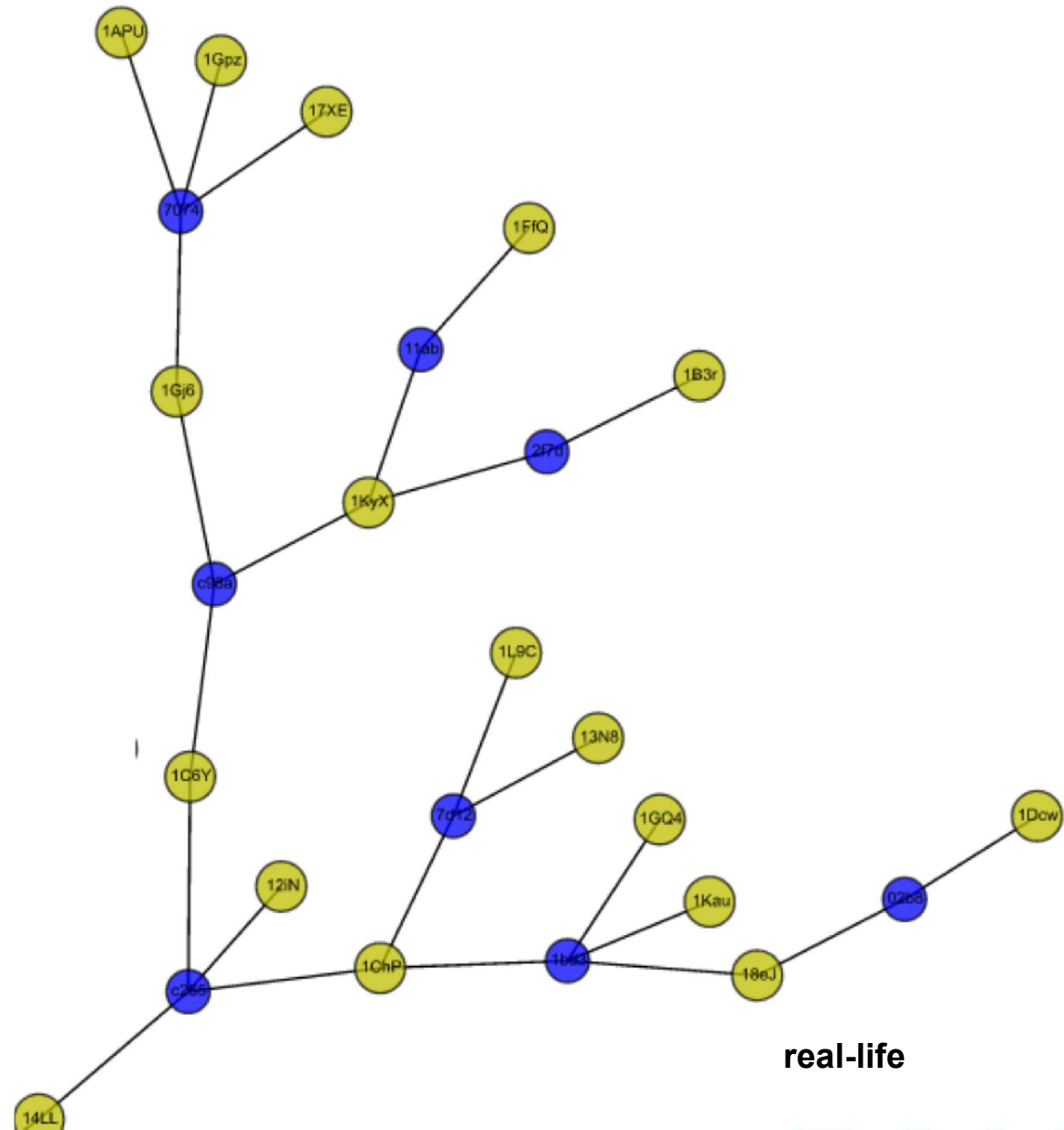
³ CloudFlare, London, UK



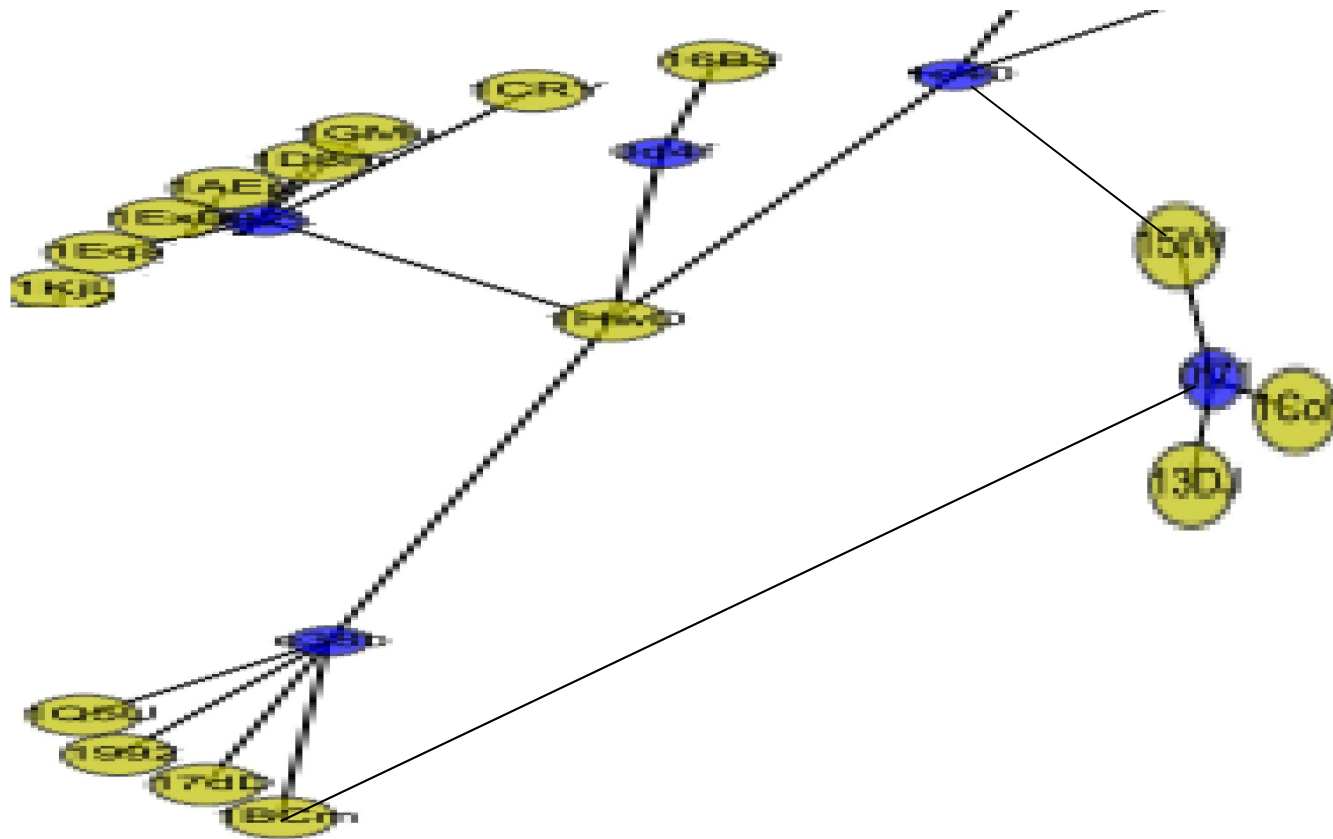
Abstract. In this paper we study the question of key management and practical operational security in bitcoin digital currency storage systems. We study the security two most used bitcoin HD Wallet key management solutions (e.g. in BIP032 and in earlier systems). These systems have extensive audit capabilities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

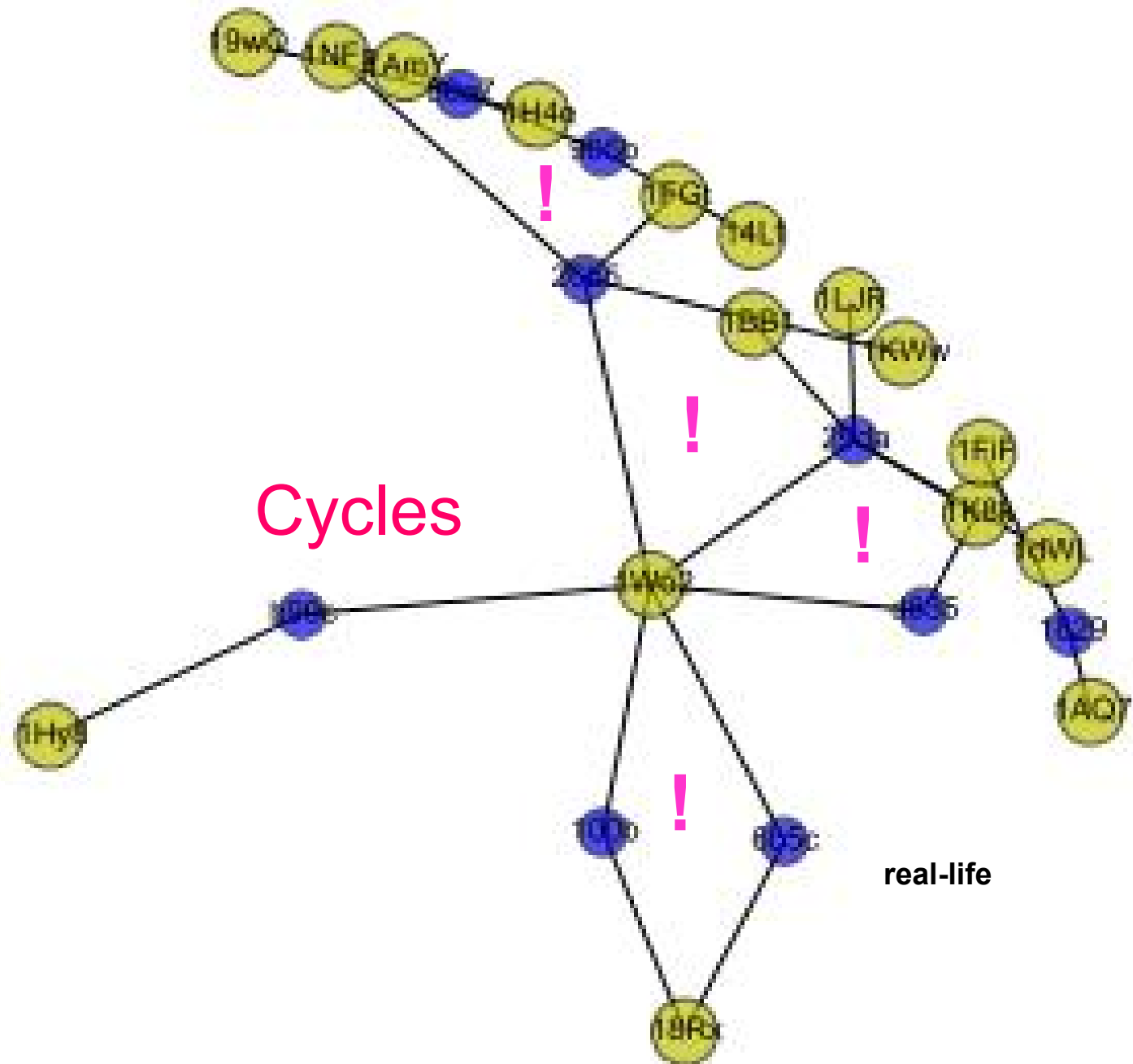
HD Wallets = Trees



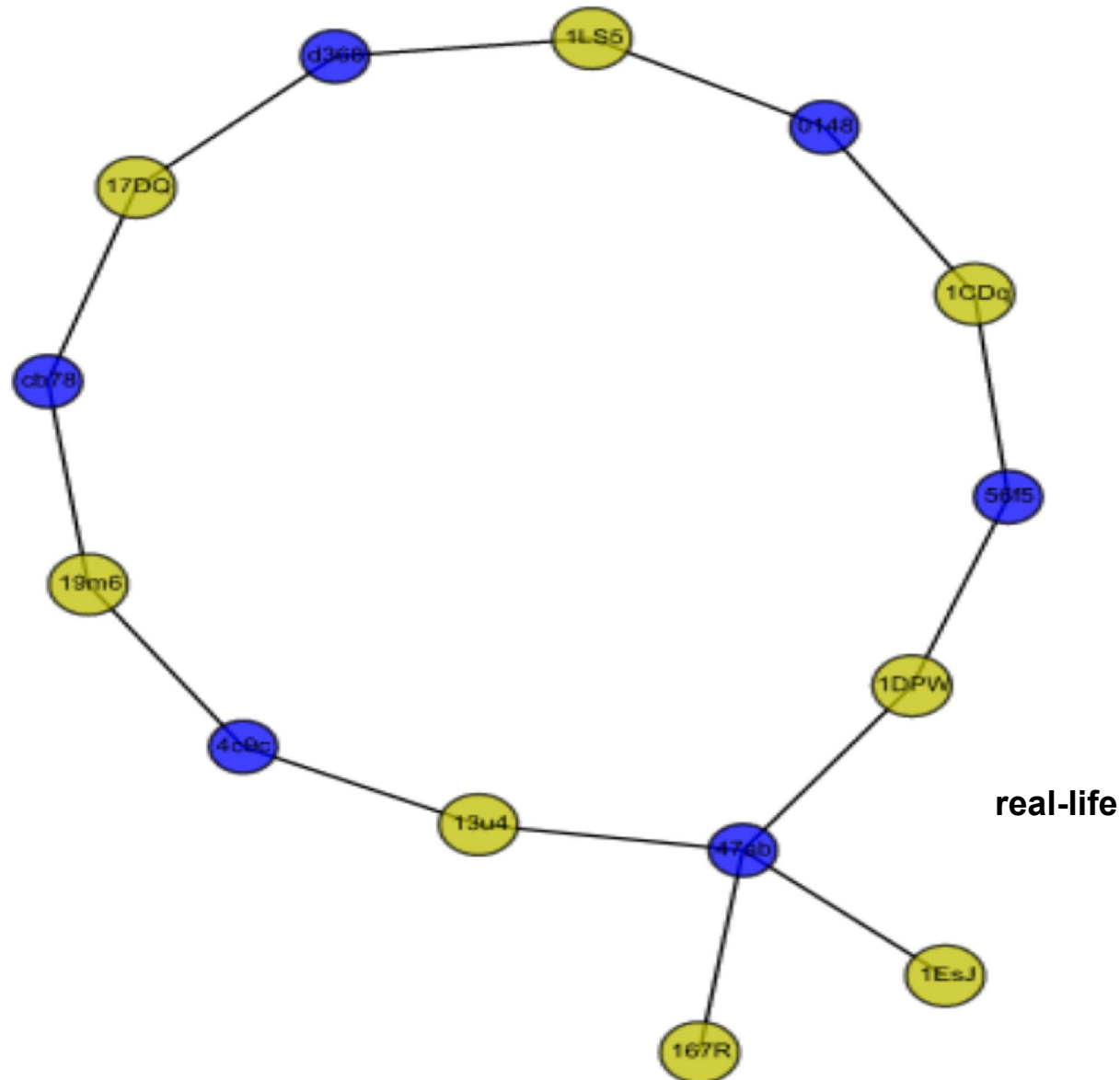
2 Trees Connected Due to Bad Randoms



contrived

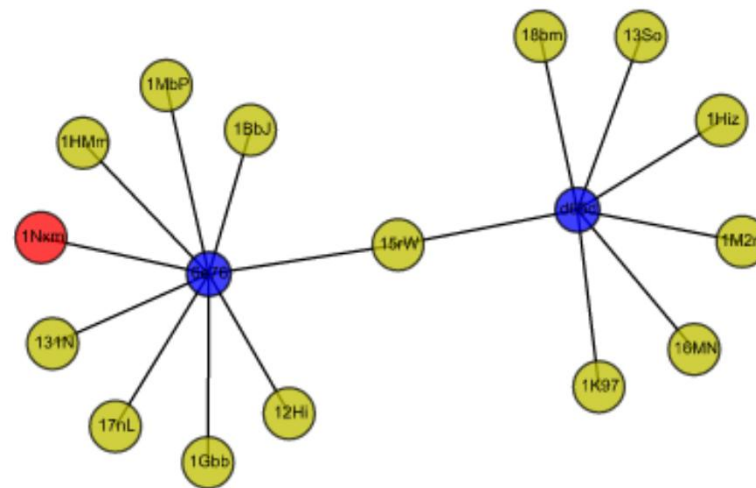


Q1: Is This One Broken???



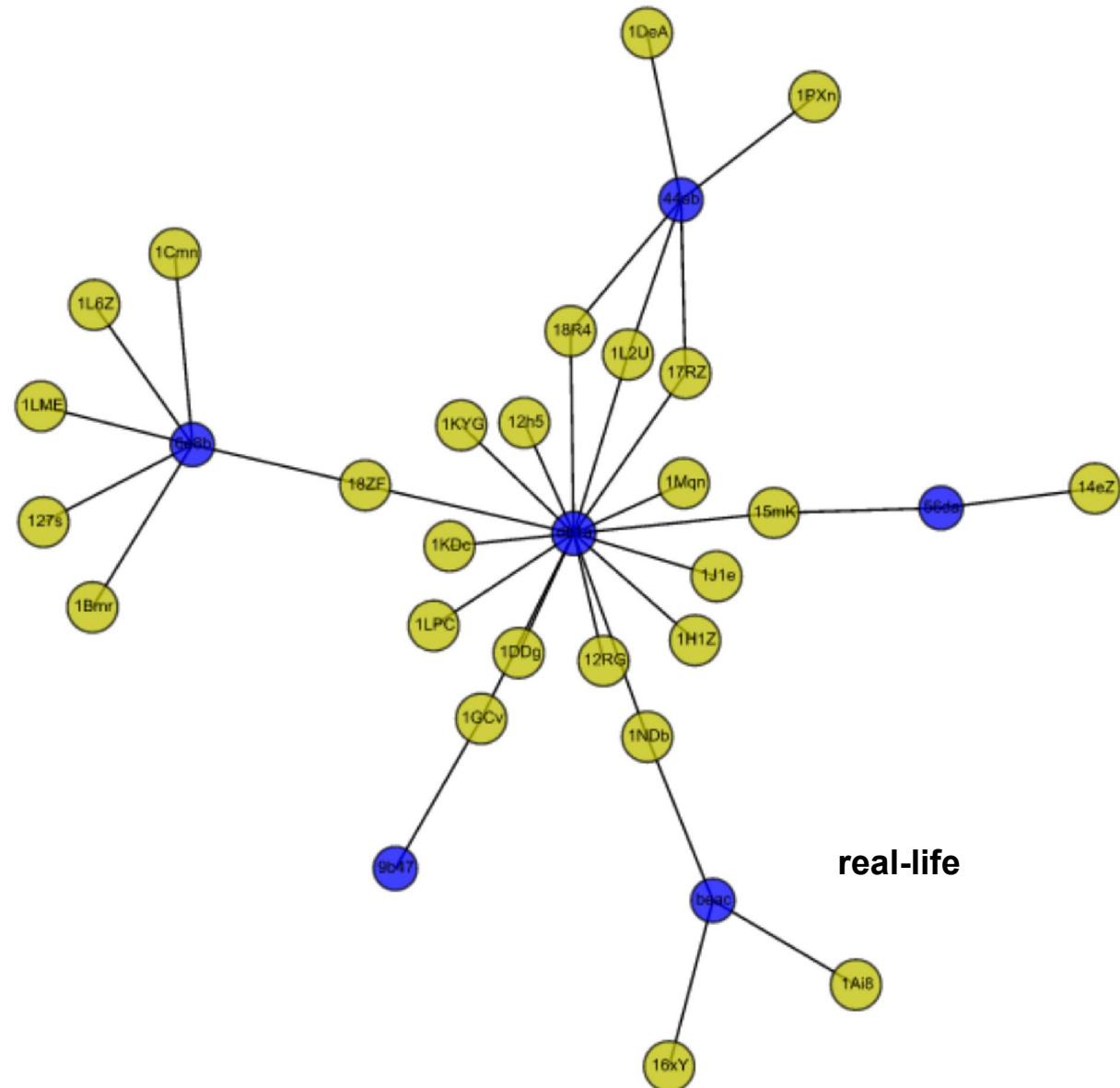
Q2: Is This One Broken???

(what is **red** colour?)

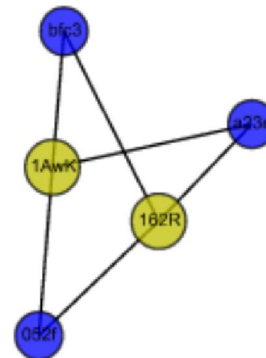
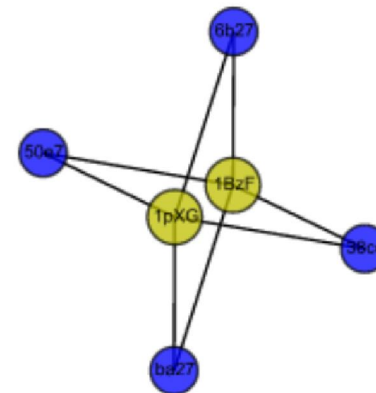
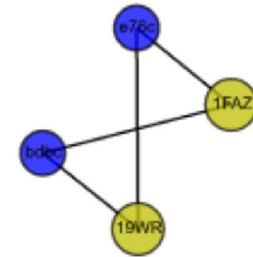
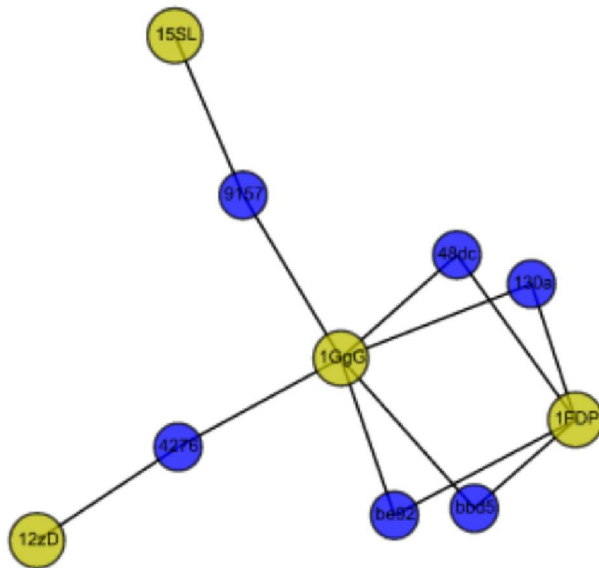


real-life

Q3: This One??? (harder)

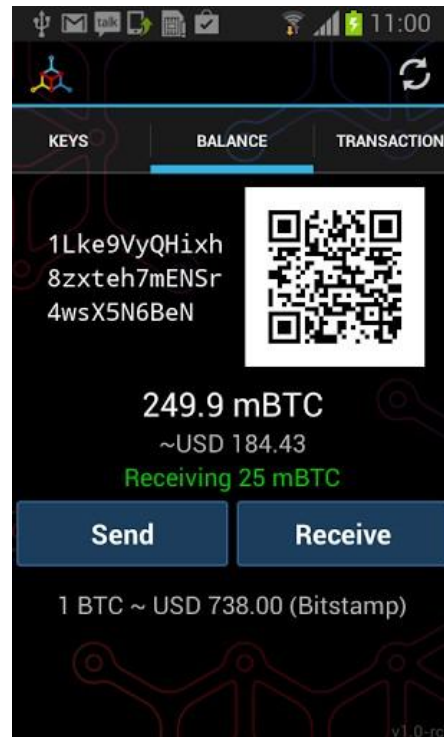


****similar examples**



real-life

Secure Storage of Bitcoins



Bottom Line

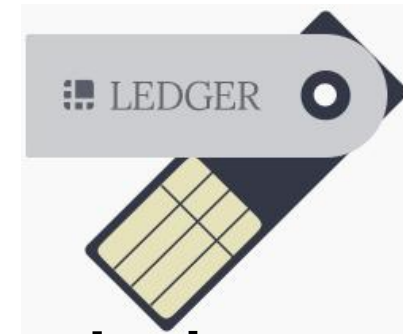
Main Functionality:

- Private Key Generation
- Export public key
- ECDSA sign



BTChip HW1

hardwarewallet.com

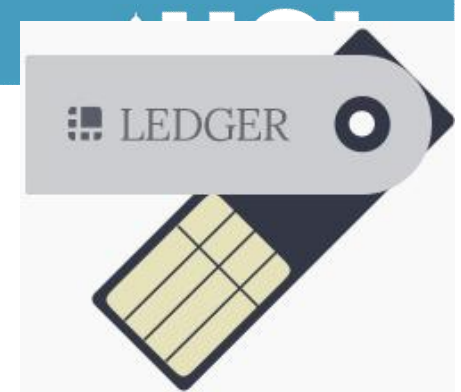


Ledger

ledgerwallet.com

Ledger Implements:

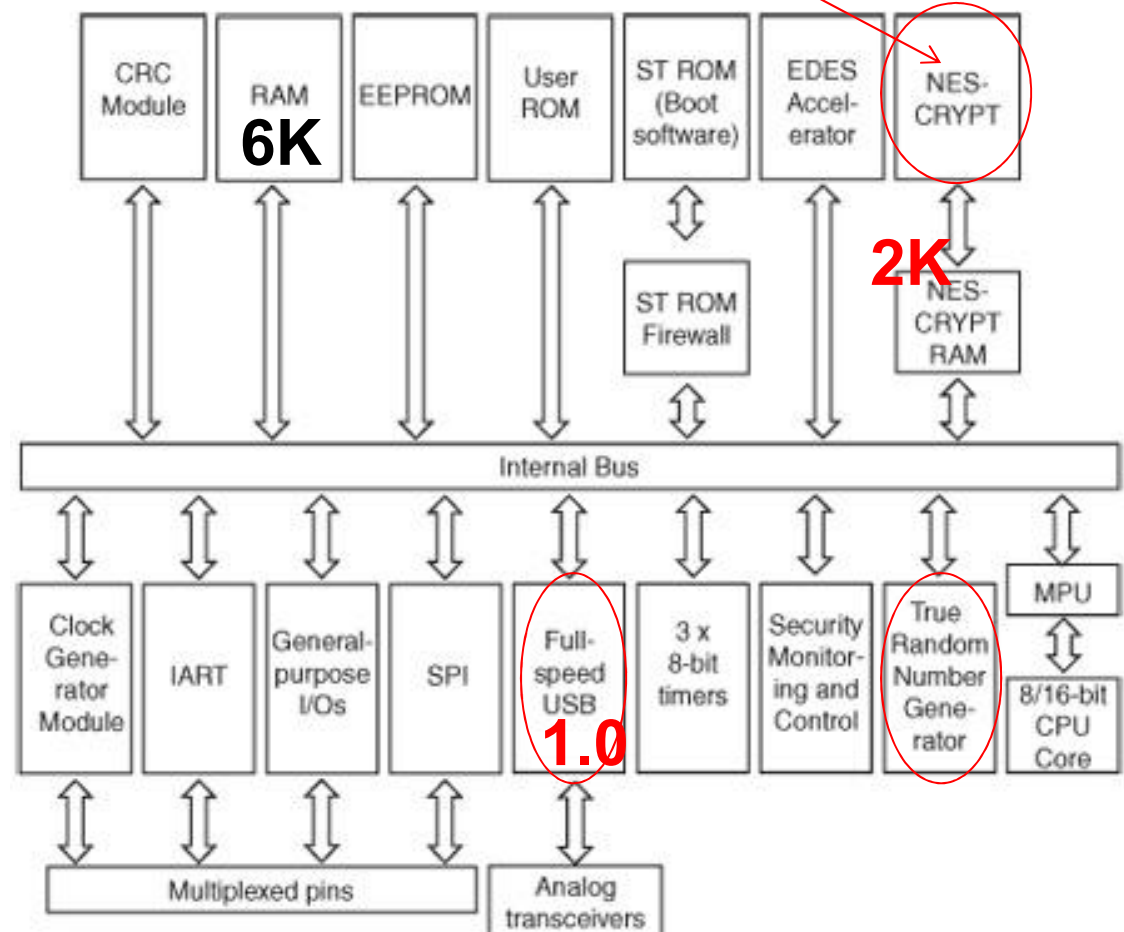
- BIP032 : HD Wallets
 - ⇒ danger, see our paper...
 - ⇒ Solution: implements RFC 6979, deterministic signatures





*Features of USB card **ST23YT66** NESCRIPT 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

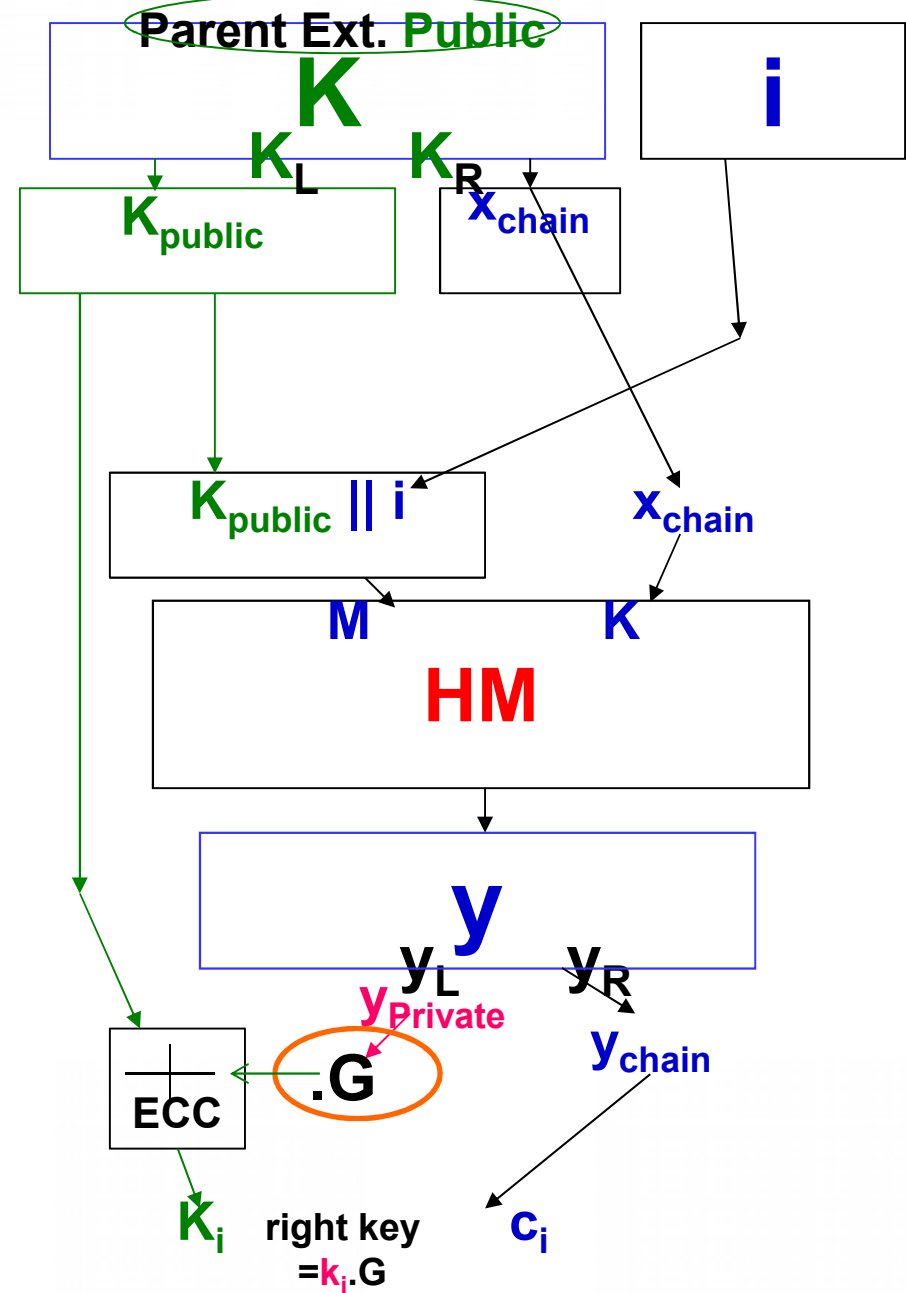
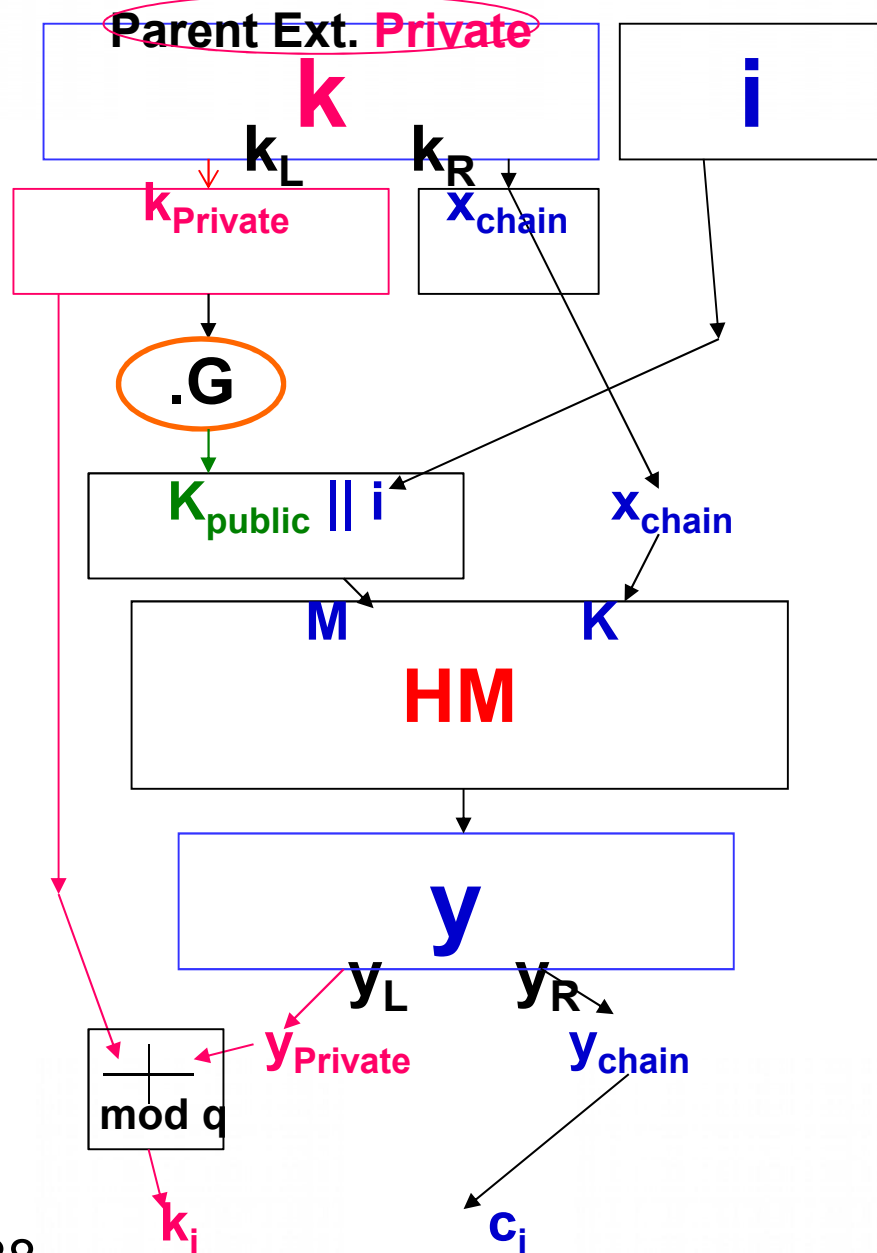
Allows to see your money
when you don't have your device with you!



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>



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.”
 - not a good idea to send these things by email...
[lower level=>smaller risk but still a key which endangers MANY private keys]



Are Known Wallet Solutions Secure?

??



Is There a Fix?

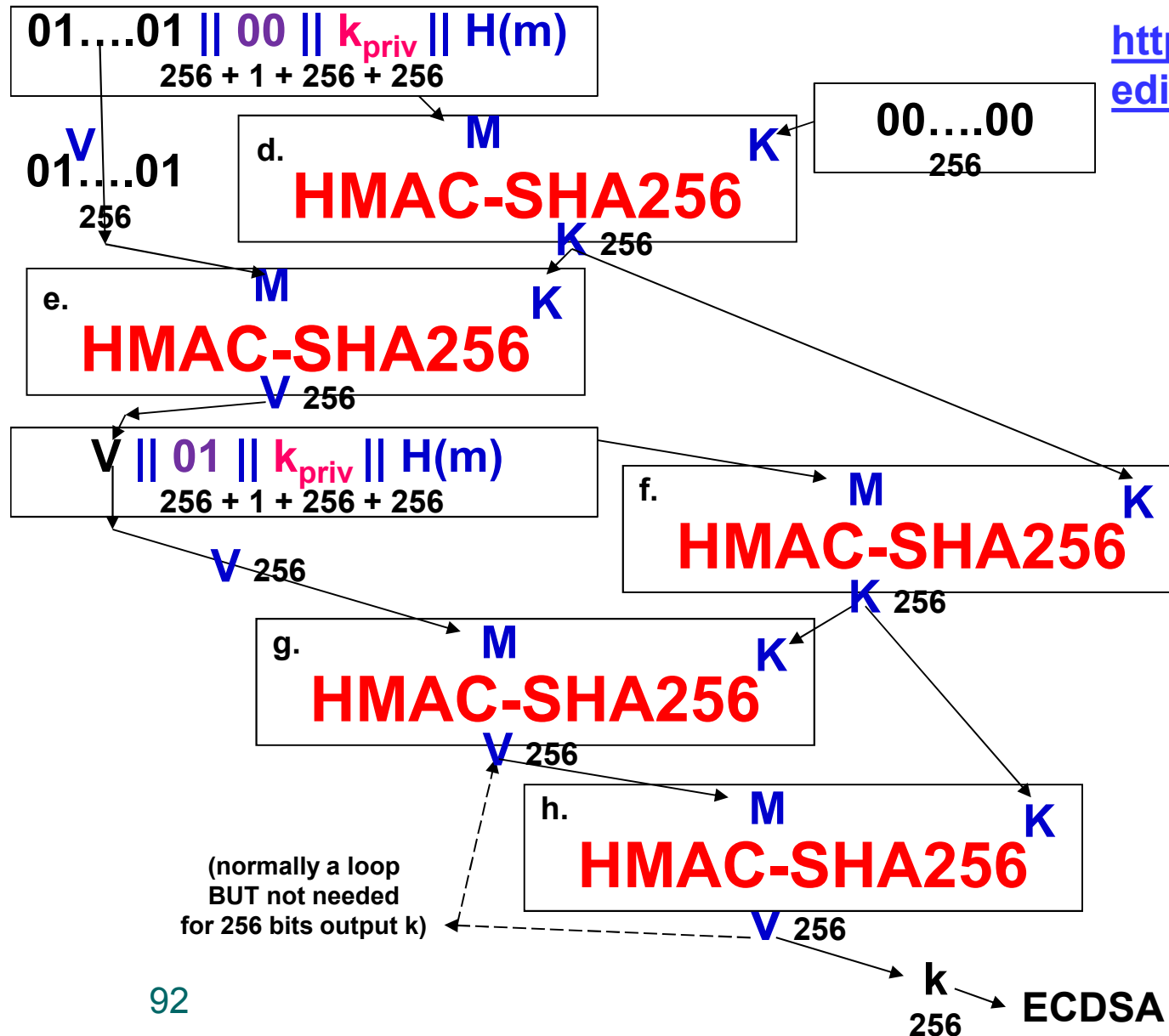
Solution: RFC6979 [Thomas Pornin]

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]

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