Cryptographic Security of ECDSA in Bitcoin

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 improve
the security baseline…

My Whole Life:

Tried to improve
the security baseline…

Crying Wolf!

51%, Elliptic Curve, OpenSSL...

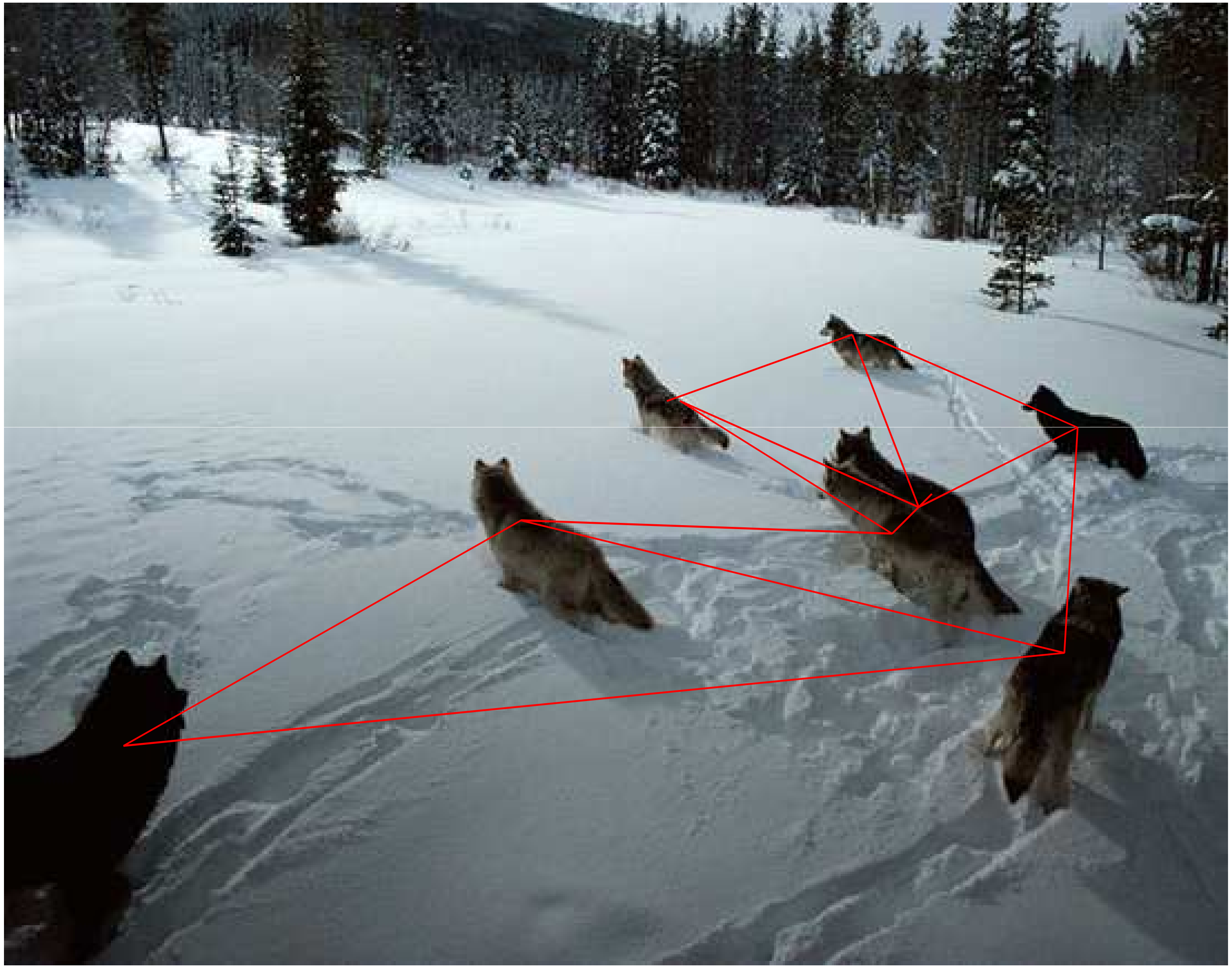
It did NOT help,

The Wolf was allowed to operate

We failed to protect our DATA

We 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?
  - 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
The coming digital anarchy

But Is Cryptography Incorruptible?

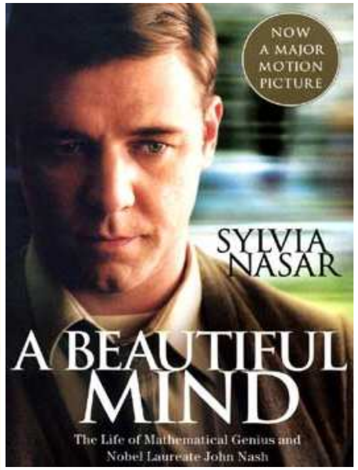
NSA 2013 Budget, excerpts:

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

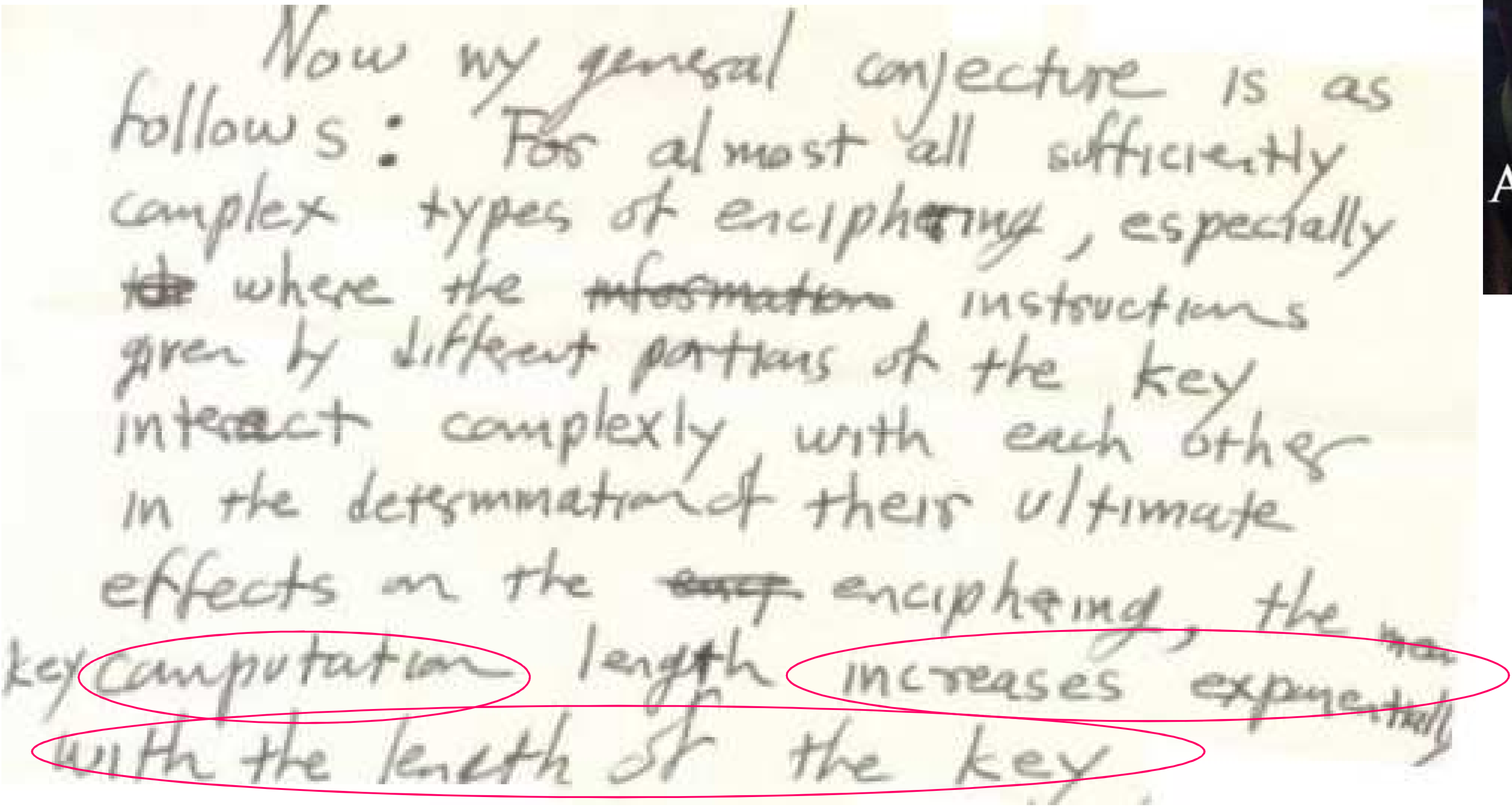
[…] Insert vulnerabilities into commercial encryption systems […]

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

John Nash - 1955



In 2012 the NSA declassified his hand-written letter:



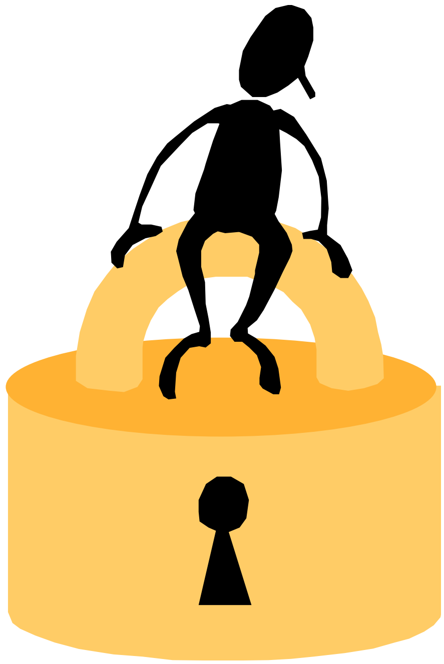
Now my general conjecture is as follows: For almost all sufficiently complex types of enciphering, especially ~~the~~ where the ~~information~~ instructions given by different portions of the key interact complexly with each other in the determination of their ultimate effects on the ~~enc~~ enciphering,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

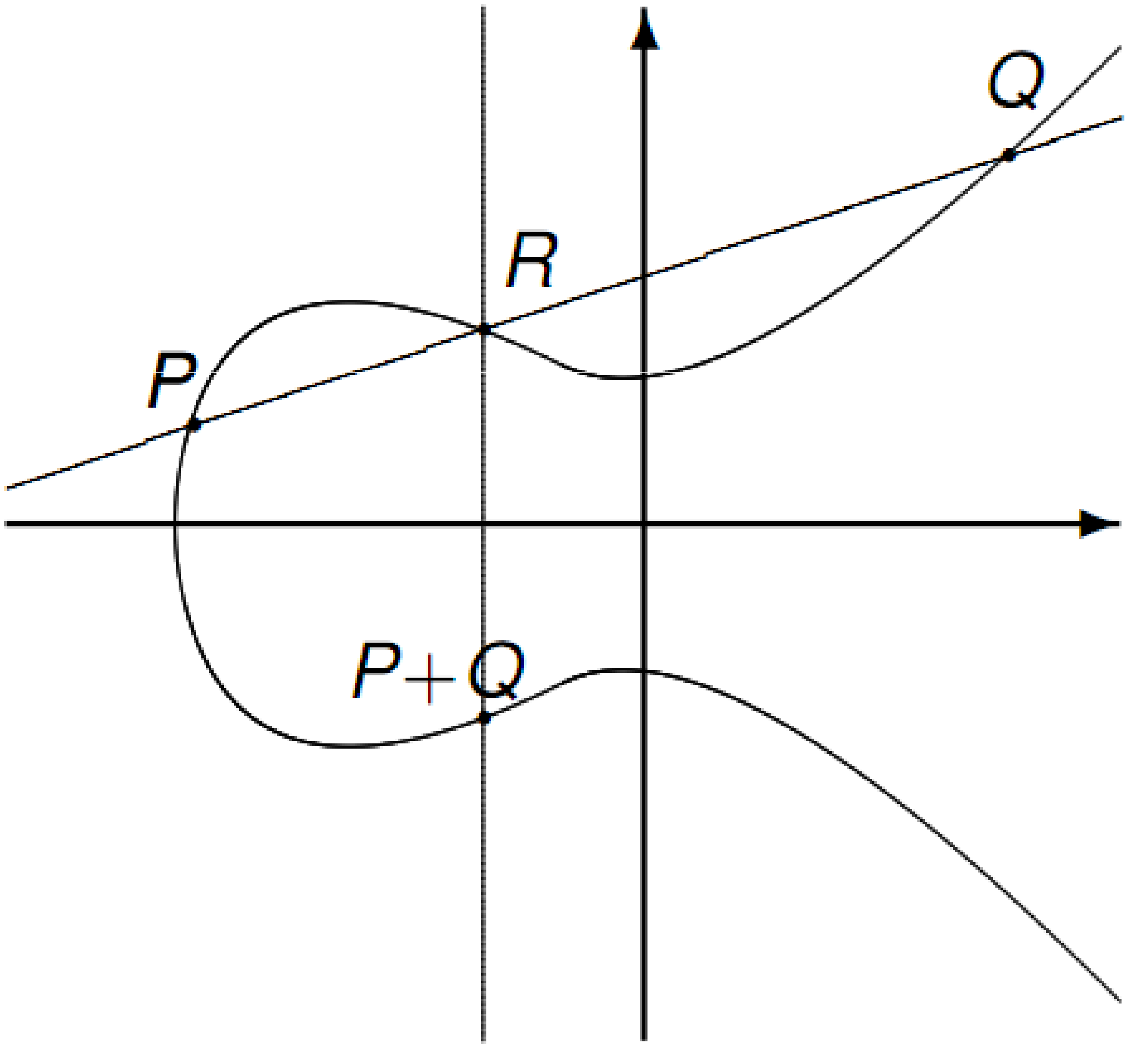
He also says that:

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

Elliptic Curve Crypto

"exponential security"





ECC - Certicom Challenges [1997, revised 2009]

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

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

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

ECCp-97	97	71982	$ 5,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECCp-109	109	9.0×10^6	$10,000
ECCp-131	131	2.3×10^{10}	$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECCp-163	163	2.3×10^{15}	$30,000
ECCp-191	192	4.8×10^{19}	$40,000
ECCp-239	239	1.4×10^{27}	$50,000
ECCp-359	359	3.7×10^{45}	$100,000

TOTAL = 725,000 USD

P vs. NP

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

How to Steal Bitcoins

New attacks [Courtois et al. October 2014]

eprint.iacr.org/2014/848/

=>more details later…

Crypto Challenges:

I always liked this idea.

Claiming (very naive) that this would:

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

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

ECC - Certicom Challenges [1997, revised 2009]

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

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

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

ECCp-97	97	71982	$ 5,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECCp-109	109	9.0×10^6	$10,000
ECCp-131	131	2.3×10^{10}	$20,000

Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECCp-163	163	2.3×10^{15}	$30,000
ECCp-191	192	4.8×10^{19}	$40,000
ECCp-239	239	1.4×10^{27}	$50,000
ECCp-359	359	3.7×10^{45}	$100,000

secp256k1

NOT INCLUDED

no price if you break it ☹

Timely Denial

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

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

September 2013,
https://bitcointalk.org/index.php?topic=289795.80

Comparison:

Used/recommended by:	secp256k1	secp256r1
Bitcoin, anonymous founder, no one to blame…	Y	
SEC Certicom Research	surprised!	Y
TLS, OpenSSL	ever used???	Y **98.3%** of EC
U.S. ANSI X9.63 for Financial Services	Y	Y
NSA suite B, NATO military crypto		Y
U.S. NIST		Y
IPSec		Y
OpenPGP		Y
Kerberos extension		Y
Microsoft implemented it in Vista and Longhorn		Y
EMV bank cards XDA [2013]		Y
German BSI federal gov. infosec agency, y=2015		Y
French national ANSSI agency beyond 2020		Y

Wanna Bet?

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

bitcoin, cryptography, SHA256, ECDSA, ECDL, secp256k1

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

betmoose.com - Totally Anonymous Bets In BTC!

FEATURED

Bitcoin Cryptography Broken in 2015

Category: Bitcoin

By NCourtois ★★★★★

Description

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

Decision Logic

SHA256, ECDSA, ECDL, secp256k1

YES

Volume:	Ƀ 0.140
# of Bets:	3

Ƀ

PAYOUT	ROI
Ƀ0.00	0%

*assumes current weight and volumes

Place Anonymously

NO

Volume:	Ƀ 0.189
# of Bets:	6

Ƀ 0.1

PAYOUT	ROI
Ƀ0.14327	43.27%

*assumes current weight and volumes

Place Anonymously

Amount?

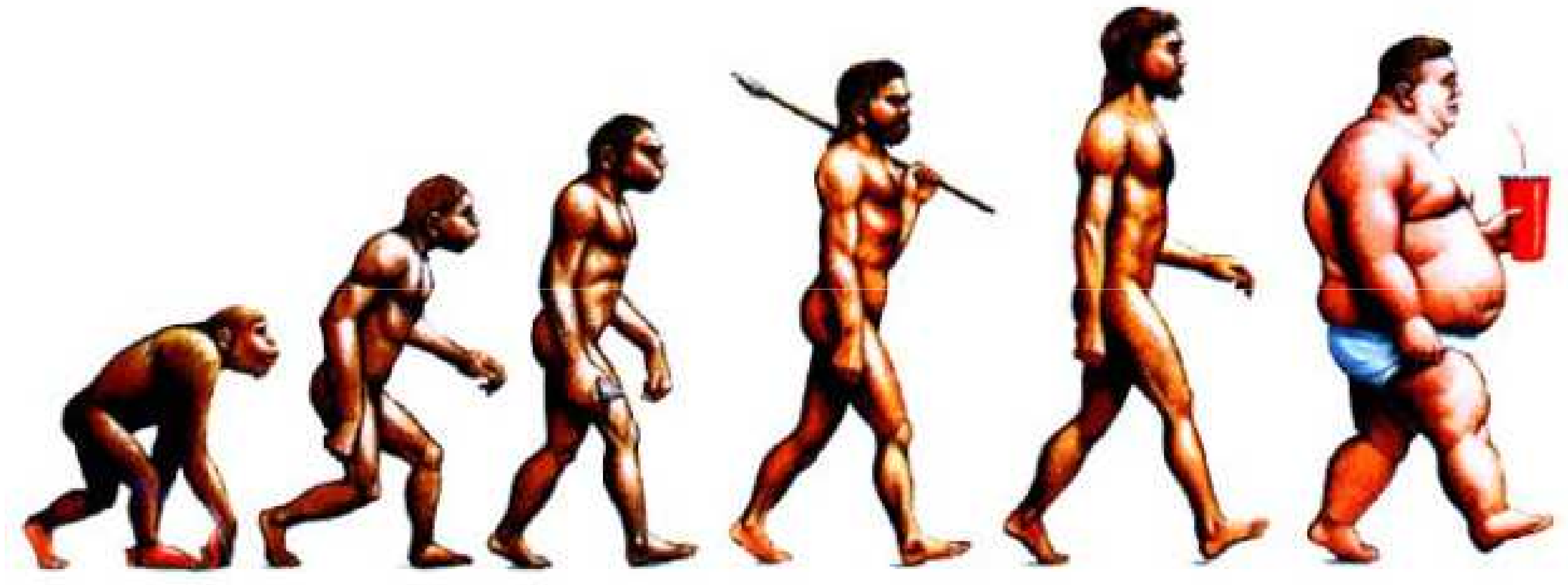
- Don’t bet a ridiculous amount!
- As long as we don’t have 2000 BTC in this bet, we will simply NOT yet know if bitcoin ECC is broken…

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

- Don’t expect that code breakers who can make 725,000 $ elsewhere, will even try to break bitcoin Elliptic Curve
- They would rather steal some bitcoins
  - Possible only if your public key is revealed

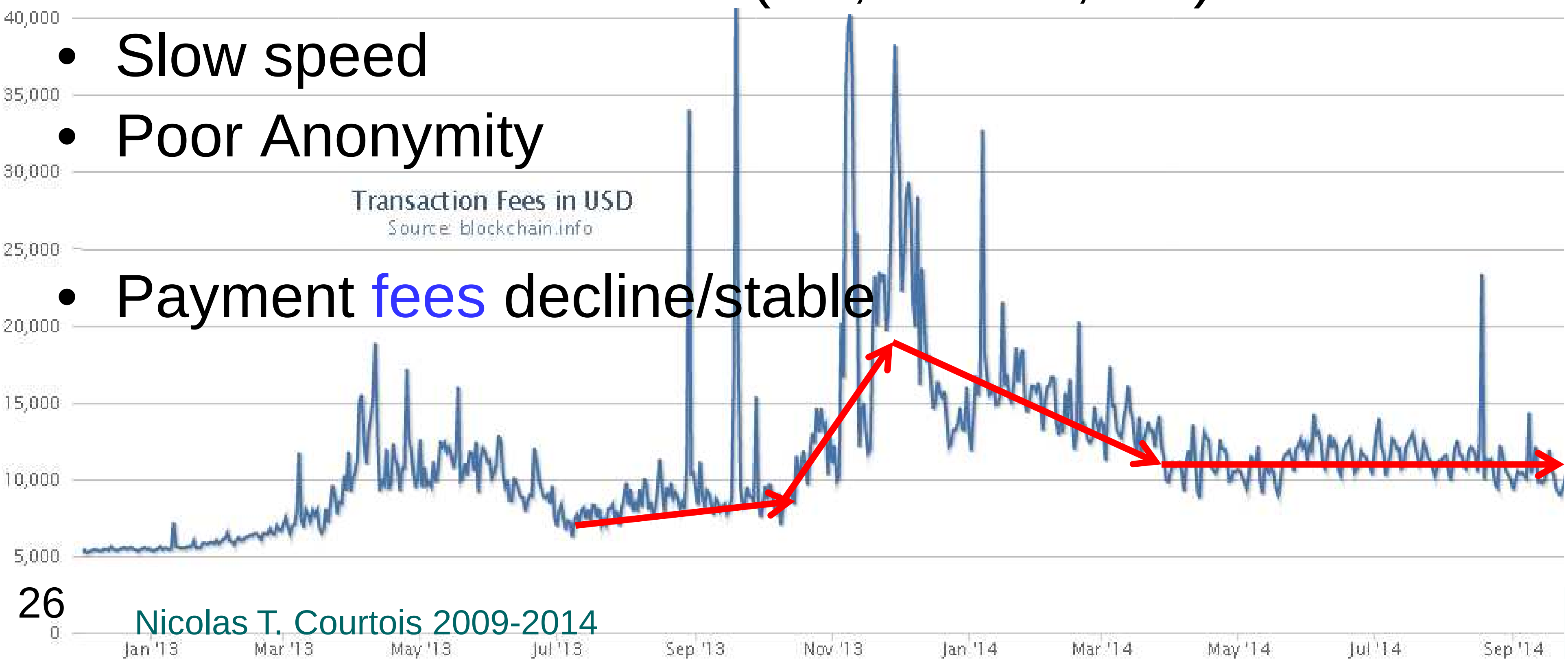
    => Tip: use each Bitcoin address only once!

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



So Far…

- Bitcoin has yet failed to achieve the most basic goal: being a decentralized P2P currency
(10 major pools control 75%)

51% Attacks

See

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

Researcher: cryptocurrencies such as Bitcoin are programmed to self destruct

Posted By: **MrFusion** [Send E-Mail]
Date: Saturday, 10-May-2014 23:05:41

Better?

- The “Yahoo of cryptocoins”
  is now waiting for
  the “Google of cryptocoins”
  to steal Bitcoin business
  purely on technical superiority
  and without a single hostile shot.

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:

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:

[Saltzer and Shroeder 1975]

1. Open design.
2. Least Common Mechanism
3. Assume that attacker controls the Internet [Dolev-Yao model, 1983].
4. The specification should be engineered in such a way that it is hard for developers to make it insecure on purpose (e.g. embed backdoors in the system).

Least Common Mechanism

Violated in Bitcoin also because it uses:

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

Open Design Principle

[Saltzer and Schroeder 1975]

Open Design ≠ Open Source

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

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/HSM…
  - 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)

Introducing Bitcoin

Bitcoin In A Nutshell

- bitocoins are cryptographic tokens, binary data = 010100110101010…
  - 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.

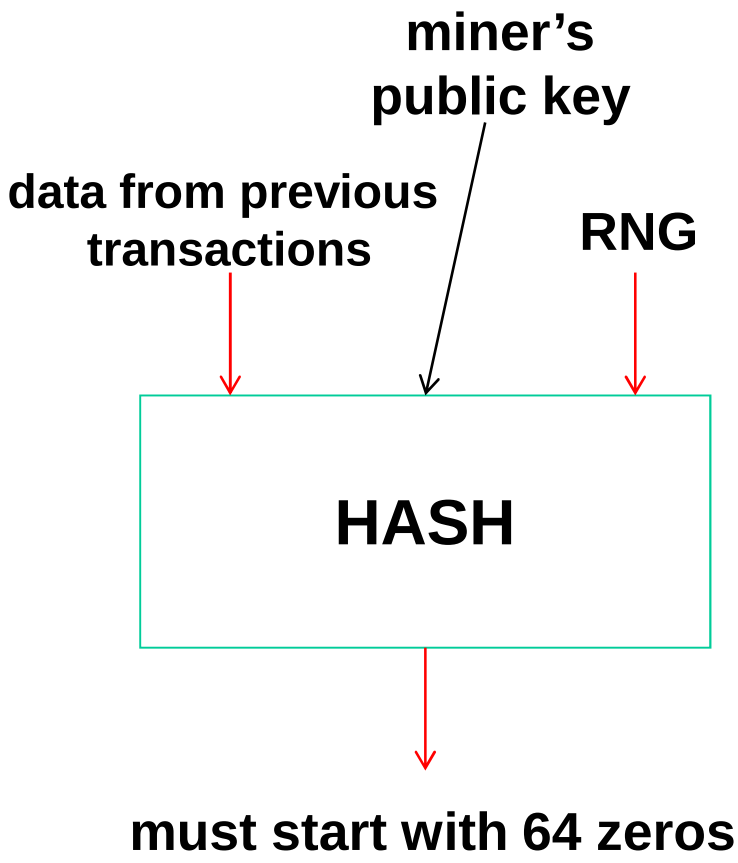
Block Chain

Bitcoin Mining

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

Ownership:

– "policed by majority of miners":



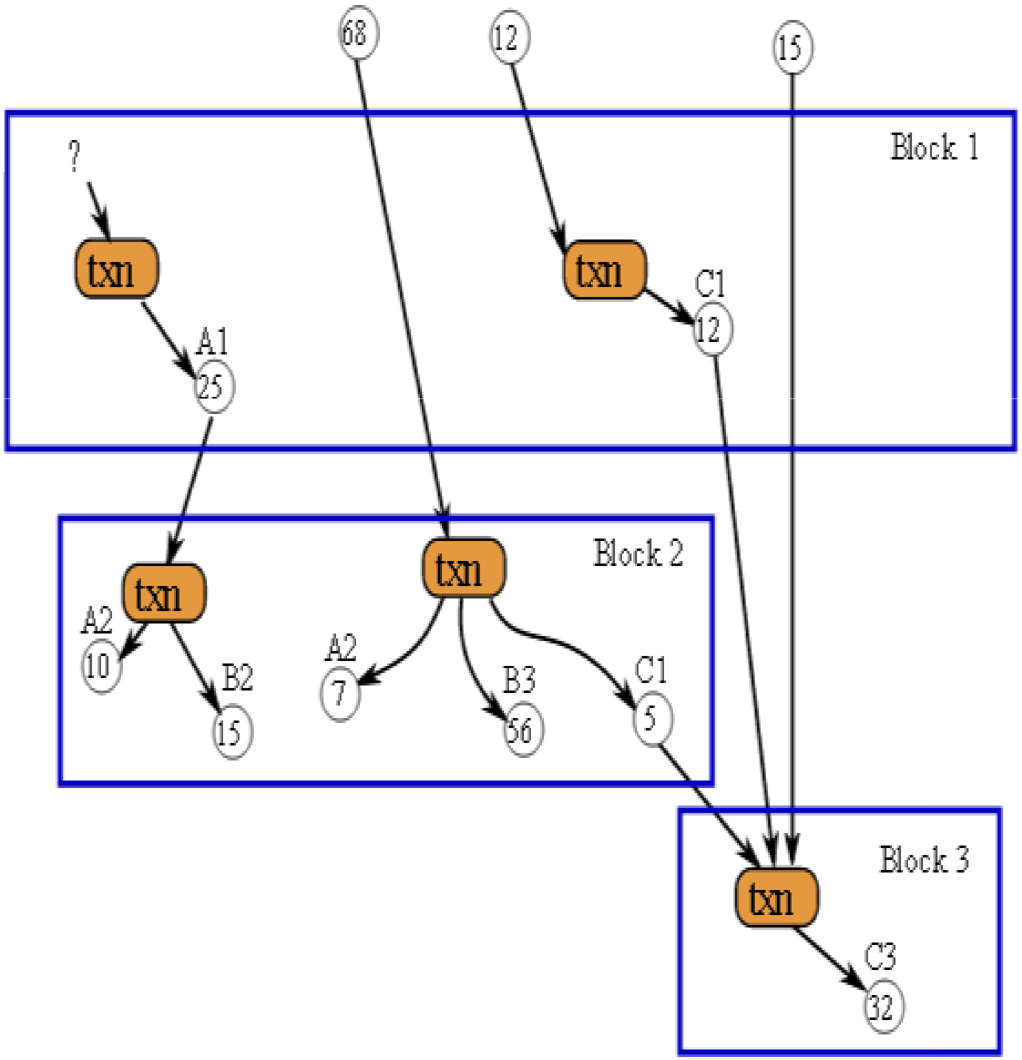
Block Chain

Def:

A transaction database
shared by everyone.

Also a ledger.

Every transaction
since ever is public.



Tx LifeCycle

- Miner nodes —**burn**→ **public ledger**

tx

- Peer Nodes

tx

- Wallet Nodes

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.

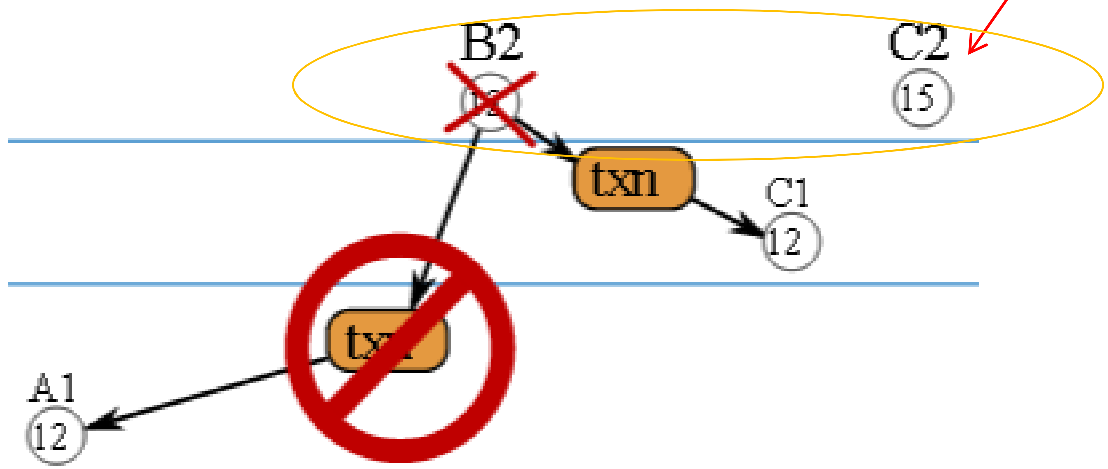
Bitcoin Ownership

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:

not spent



*Multi-Signature Addresses

Special Type of Addresses

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

The keys can be stored on different devices (highly secure).

2 out of 3 are also already implemented in bitcoin.

(1 device could be absent, money can still be used).

Very cool, solves the problem of insecure devices…

Adding Another Layer Of Security

MultiSig:

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

Multi-Sig Concept is NOT new…

1993

Efficient multi-signature schemes for cooperating entities

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

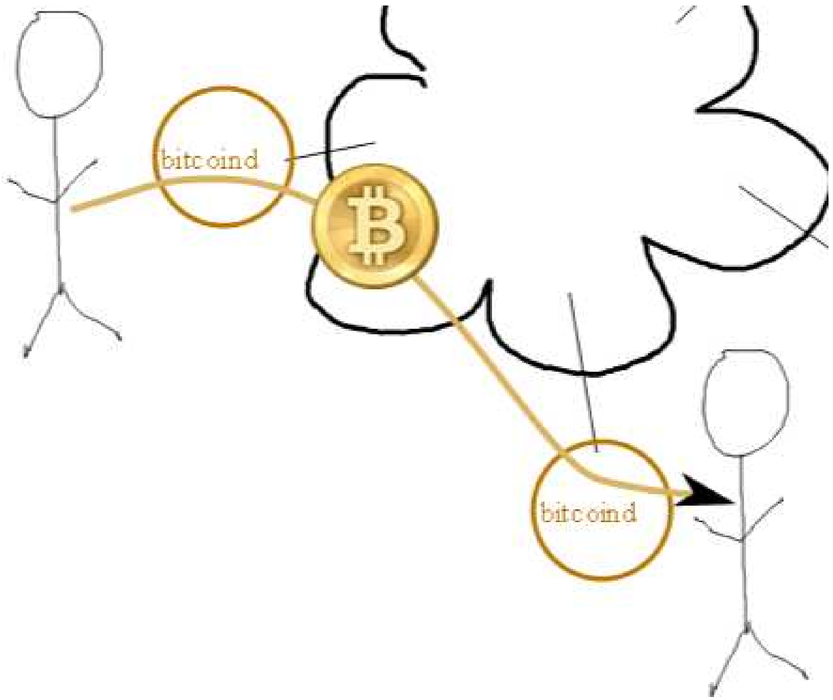
Bitcoin Circulation

Bitcoin Transactions:

- between any two addresses [and any two network nodes],
  - at any time [no market closing hours].
  - validated within 10-60 minutes.
    - should wait longer for larger transactions, beware of “cheating miners”…
    - 0-confirmation =
      - many websites accept instantly,
      - they trust your application not to double spend
      - and trust miners to reject the second spent based on later time and wider circulation, quite plausible!

Transfer


To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi3
Amount: 1.0 BTC
SEND

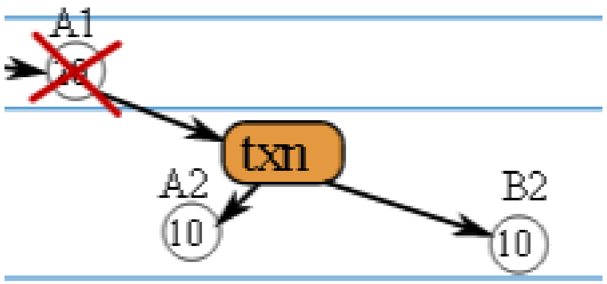

bitcoind
bitcoind

In / Out

Owner of a certain "Attribution to PK" can at any moment transfer it to some other PK addresses.

=> 0 inputs possible if minting transaction… new money.

=> Several outputs are a norm for bitcoin transactions.

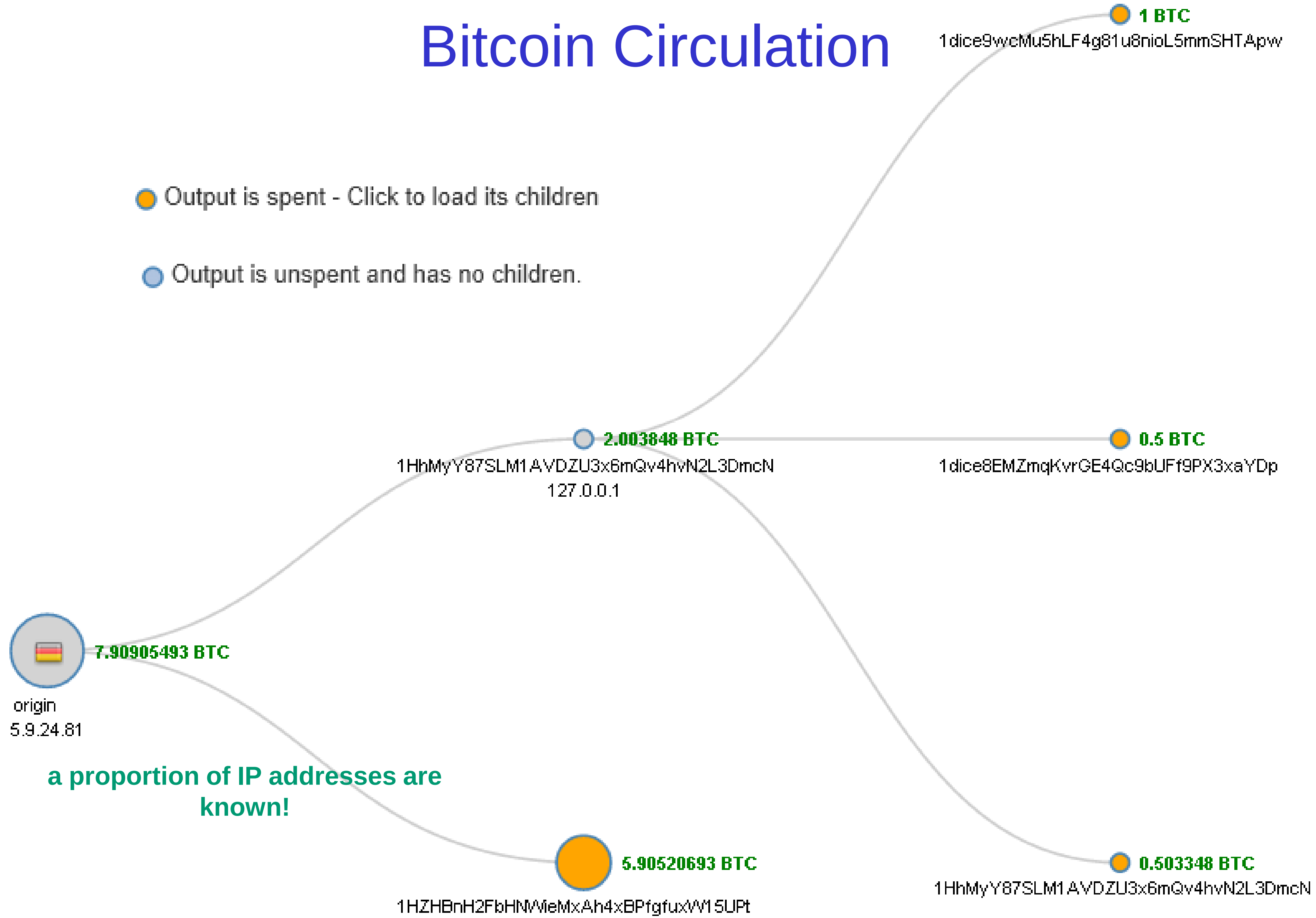


on this picture we ignore the fees

Bitcoin Transfer

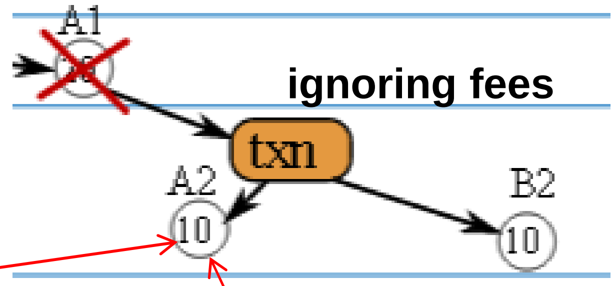
Owner of a certain “Attribution to PK” can at any moment transfer it to any other PK address.

Bitcoin Circulation



a proportion of IP addresses are known!

Attributions



DEFINITION

"Attribution to PK" =

act of an owner of
a previous attribution (always destroyed)
which transfers a certain amount to the new PK = A2

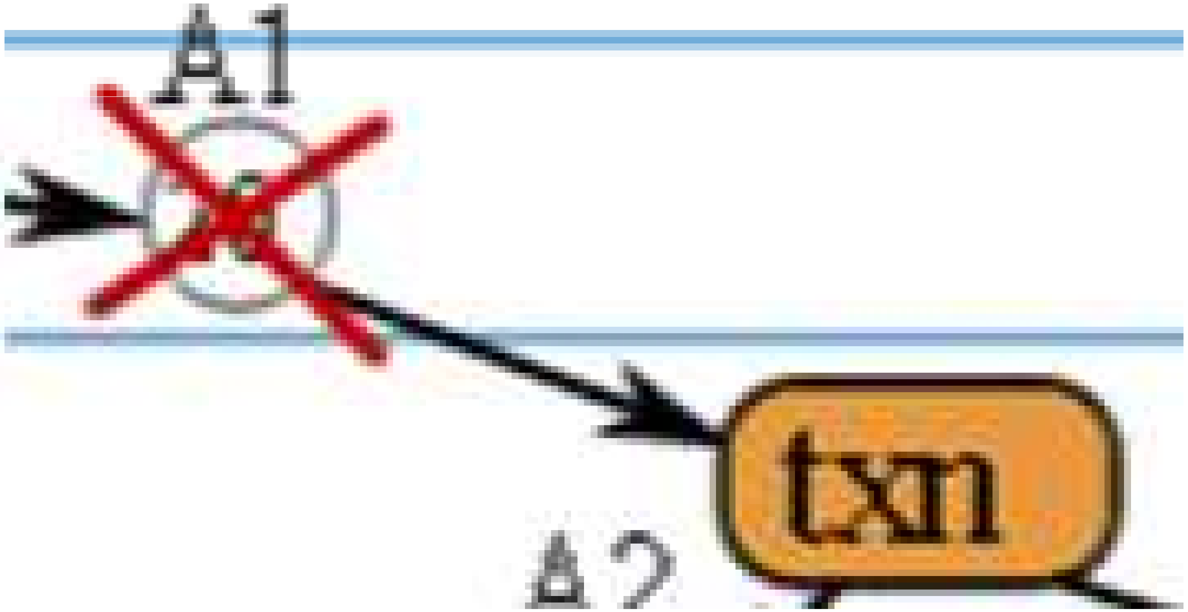
(using a digital signature)

Caveat: Each attribution can be traced back to the initial mining event.

Fragmentation and Summation Rule

Each PK has a balance, say 20 BTC
current balance = sum(unspent attributions).

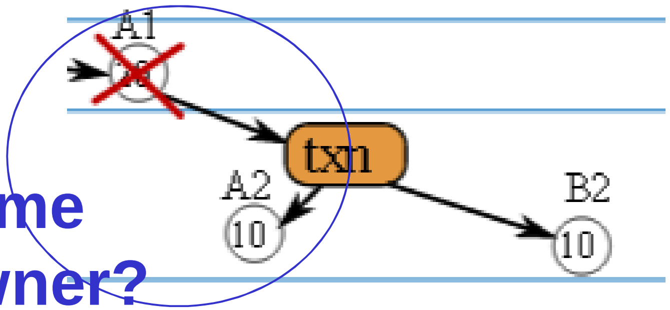
Attributions are ALWAYS destroyed when used,



From Single Attribution

Example

- Change: return some money to ourselves inside the same transaction
  - this implies most transactions have 2 or more outputs
  - most apps use the same address
  - could use another fresh address for better anonymity, but too lazy…



same owner?

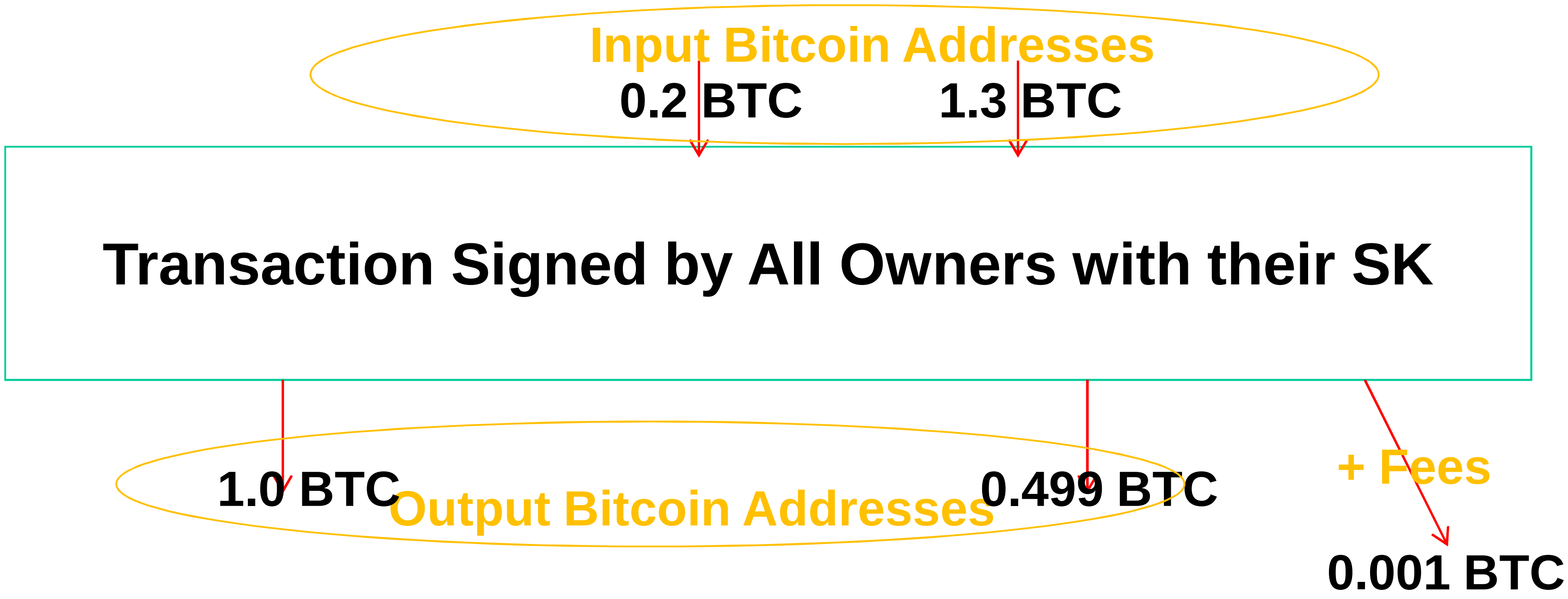
no way to know for sure…

With Multiple Attributions

typical case, even for a single user

Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.

- helps for anonymity.
- destroys all current attributions,
- requires everybody's signature

can repeat, specifies
tx origin +index of each!

Input Bitcoin Addresses

0.2 BTC 1.3 BTC

Transaction Signed by All Owners with their SK

The transaction is signed but invalid to start with, it becomes valid only when confirmed many times by other people (embedded in a new block)

0 1

1.0 BTC 0.499 BTC

Output Bitcoin Addresses

+ Fees

0.001 BTC

frequently repeat some input addresses
could all belong to the same person

https://blockchain.info/tx/99929d9ad149047ae79998592241dddf7ef4ae2f4bb4e057e9c36c4cefa88830

Home Charts Stats Markets Developers Wallet

Example 1

Transaction View information about a bitcoin transaction

99929d9ad149047ae79998592241dddf7ef4ae2f4bb4e057e9c36c4cefa88830

1EWJJCnBuyQDPwVHuCycUCMHCVxTSGLBvk
1MisJY7KwjnhmdaMwyH6v1A3jDQpty7rdg

1BaQzo1SyRXZRhQwSvsQJKAUvi5tu3L9uQ	10 mBTC
1rpU1Wa3pYeuJEbRPMWDDCxeh5PDMBrQ9	83.50001 mBTC
1BSy1ARBQfT9PRDYYB6DvzRkbSVRgbaX3	1.39661 mBTC

94.89662 mBTC

can repeat, tx origin + index of each is included in the rawtx

can repeat input addresses

Summary	
Size	471 (bytes)
Received Time	2013-07-20 19:00:32
Included In Blocks	247599 (2013-07-20 19:03:29 +3 minutes)
Confirmations	3712 Confirmations
Relayed by IP	5.164.198.173 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	95.39662 mBTC
Total Output	94.89662 mBTC
Fees	0.5 mBTC
Estimated BTC Transacted	94.89662 mBTC
Scripts	Show scripts & coinbase

Example 2 = Raw Transaction

unique ID on 256 bits = the hash of the whole

list of input attributions: origin tx, **index n**, ECDSA signature

list of output attributions

amount BTC

```
{
  "hash":"9837485da283ce8ceb0570e2950bb65ebacef9ebd97f871da268d73ea79292c4",
  "ver":1,
  "vin_sz":1,
  "vout_sz":2,
  "lock_time":0,
  "size":257,
  "in":[
    {
      "prev_out":{
        "hash":"ba250a395cf37e2d112859ec1d4379a605a6fd8e96b406c4f69901abc05d5b47",
        "n":1
      },
      "scriptSig":"304402206dcf0ef7ca4bfa573ed8f3dc94dca42f5ea46827e8885056d3dfede88e52d49b022077055f3d3c125cc
    }
  ],
  "out":[
0   {
      "value":"5.00000000",
      "scriptPubKey":"OP_DUP OP_HASH160 dcc1120deb91acda0d3e5774a2b8908e3424f532 OP_EQUALVERIFY OP_CHECKSIG"
    },
1   {
      "value":"13.07598401",
      "scriptPubKey":"OP_DUP OP_HASH160 88f1271342d5f2202995c6e74ed07b81caec7633 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
},
```

H(recipient PK)

Remarks:

About XX million transactions ever made.

To know the balance of one account, we must “in theory” store ALL the transactions which send money for this address and then check ALL transactions made since then to see some of these are not already spent.

Full bitcoin network nodes stored all transactions ever made and checks their correctness (all the digital signatures).

About 24 Gbytes data, 48 hours typical download.

In practice one could skip check for things confirmed by many miners… dangerous though. There is no absolute proof that miners have already checked them (maybe they forgot, a bug).

Transaction Scripts

***Scripts

Signature Script

list of output attributions

0

1

H(recipient PK)

Redemption Script

```
{
  "hash":"9837485da283ce8ceb0570e2950bb65ebacef9ebd97f871da268d73ea79292c4",
  "ver":1,
  "vin_sz":1,
  "vout_sz":2,
  "lock_time":0,
  "size":257,
  "in":[
    {
      "prev_out":{
        "hash":"ba250a395cf37e2d112859ec1d4379a605a6fd8e96b406c4f69901abc05d5b47",
        "n":1
      },
      "scriptSig":"304402206dcf0ef7ca4bfa573ed8f3dc94dca42f5ea46827e8885056d3dfede88e52d49b022077055f3d3c125cc
    }
  ],
  "out":[
    {
      "value":"5.00000000",
      "scriptPubKey":"OP_DUP OP_HASH160 dcc1120deb91acda0d3e5774a2b8908e3424f532 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value":"13.07598401",
      "scriptPubKey":"OP_DUP OP_HASH160 88f1271342d5f2202995c6e74ed07b81caec7633 OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
},
```

Spot On Signatures

Signed Tx / Final Tx

byte by byte (similar but <u>not</u> 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, e.g. 25=0x19 or 138=0x8A**
	scriptSig	script containing signature **scriptSig**
	sequence	ff ff ff ff
output count		01
output	value	62 64 01 00 00 00 00 00 **(in Satoshis)**
	script length	**scriptPubKey length 1 byte, e.g. 25=0x19**
	scriptPubKey	script containing destination address **scriptPubKey**
block lock time		00 00 00 00 **(never used so far)**

2 scripts will be detailed later

len(1i/1o)= 223=4+1+32+4+1+ 1+71+ 1+65+ 4+1+8+ 1+25+4

First scriptSig

It is scriptPubKey BUT copied from the previous transaction (peculiarity)

len= 25=3+20+2 typically

UCL

Second scriptSig

sign+PKey

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

scriptSig

PUSHDATA 47		47	
	sequence	30	
	length	44	**scriptSig1**
	integer	02	
signature (DER)	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	
	type	04	**scriptSig2**
public key	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	

Is Bitcoin Secure?

Satoshi claimed it is…

Incidents at Operation:

Bad Randoms

Bad Randoms

First publicized by Nils Schneider:

28 January 2013

D47CE4C025C35EC440BC81D99834A624875161A26BF56EF7FDC0F5D52F843AD1

$\Rightarrow$ 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.

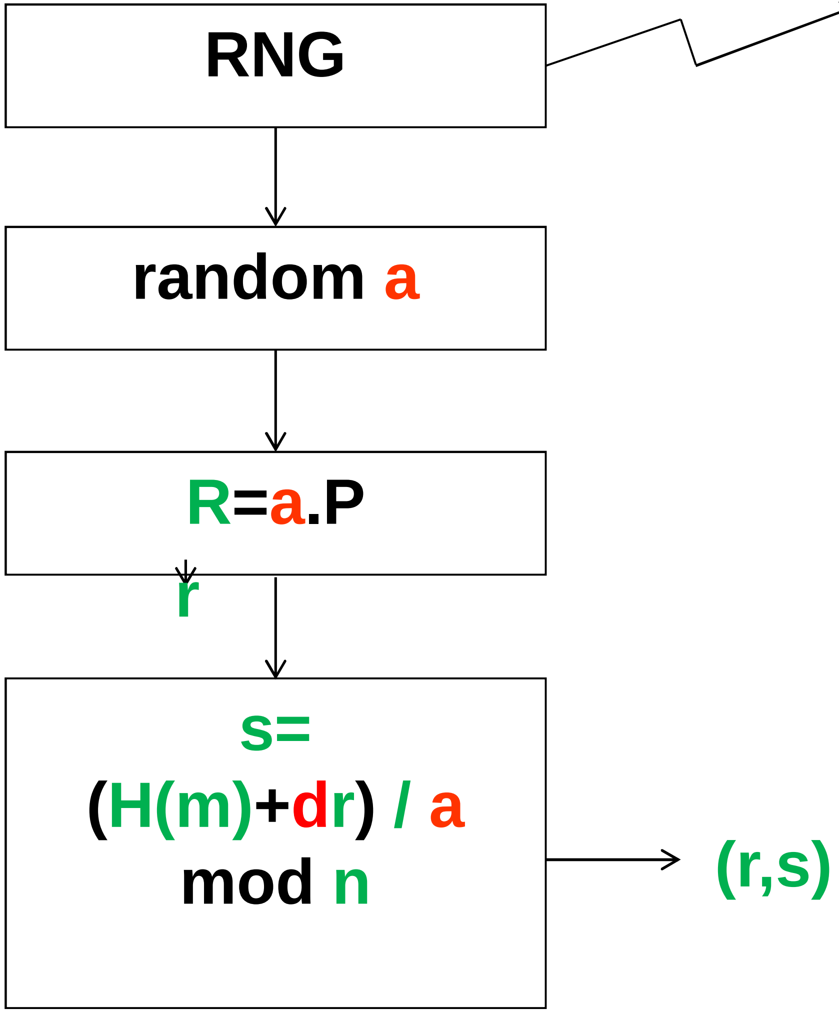
- Pick a random non-zero integer **0<a<n-1**.
- Compute **R=a.P**, where **P** is the base point (generator).
- Let **r** = (a.P)$_x$ be its x coordinate.
- Let **s = (H(m) + d*****r) / a mod n** .

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

(512 bits in bitcoin)

Attack – 2 Users

random a: must be kept secret!



has already happened 100 times in Bitcoin

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

Attack – Same User

random a: must be kept secret!

RNG

random a

R=a.P

r

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

(r,s)

has also happened 100 times in Bitcoin

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

$\Rightarrow a = (H(m_1) - H(m_2))/(s_1 - s_2) \bmod n$ AND now

$d = (sa - H(m))/r \bmod n$

anybody can steal the bitcoins!

Stopped in August 2013

Android bug was fixed…

Dec. 2013

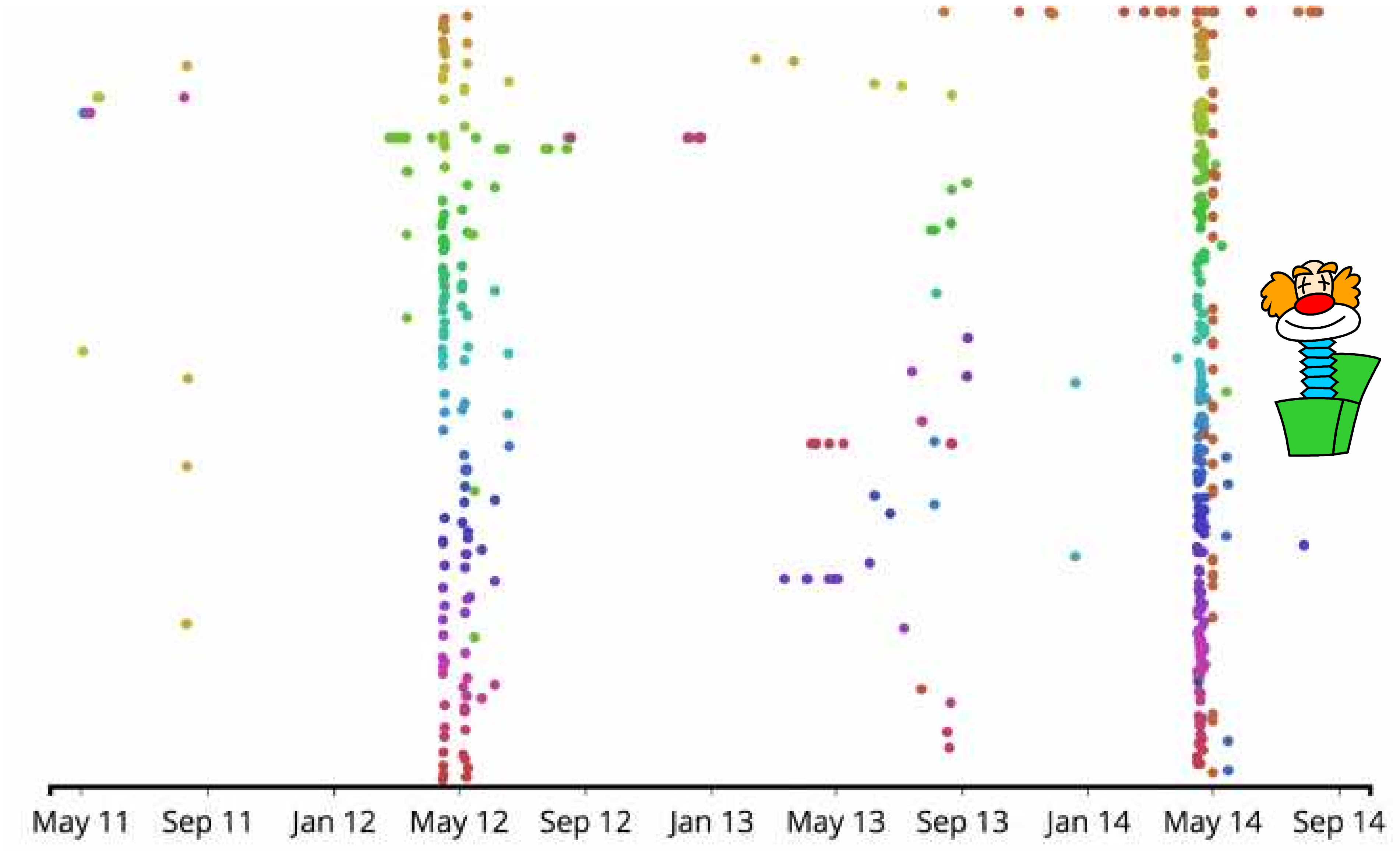
At 30C3 conference in Germany on 28 Dec 2013 Nadia Heninger have reported that they have identified a bitcoin user on the blockchain which has stolen some 59 BTC due to these bad randomness events,

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



Recent Bad Randoms

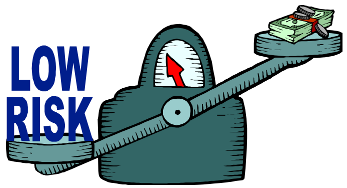
From my own scan:

0f25a7cc9e76ef38c0feadcfa5550c173d845ce36e16bde09829a3af57097240.

Appears 8 times in block 322925

28 September 2014

Used by different users…

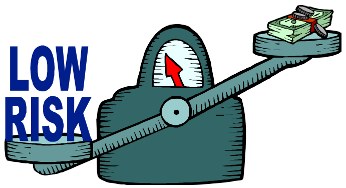


So What?

Previous attacks:

- Classical bad random attacks typically concern only very few bitcoin accounts, and only some very lucky holders of bitcoins can actually steal other people's bitcoins.

- Only a few hundred accounts in the whole history of bitcoin are affected.

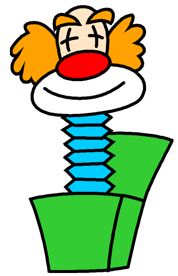


The Really Scary Attacks

New attacks [Courtois et al. October 2014]

=> under certain conditons
ALL bitcoins in cold storage
can be stolen

=>millions of accounts potentially affected.



New Paper:

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

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

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

cf.

eprint.iacr.org/2014/848/

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

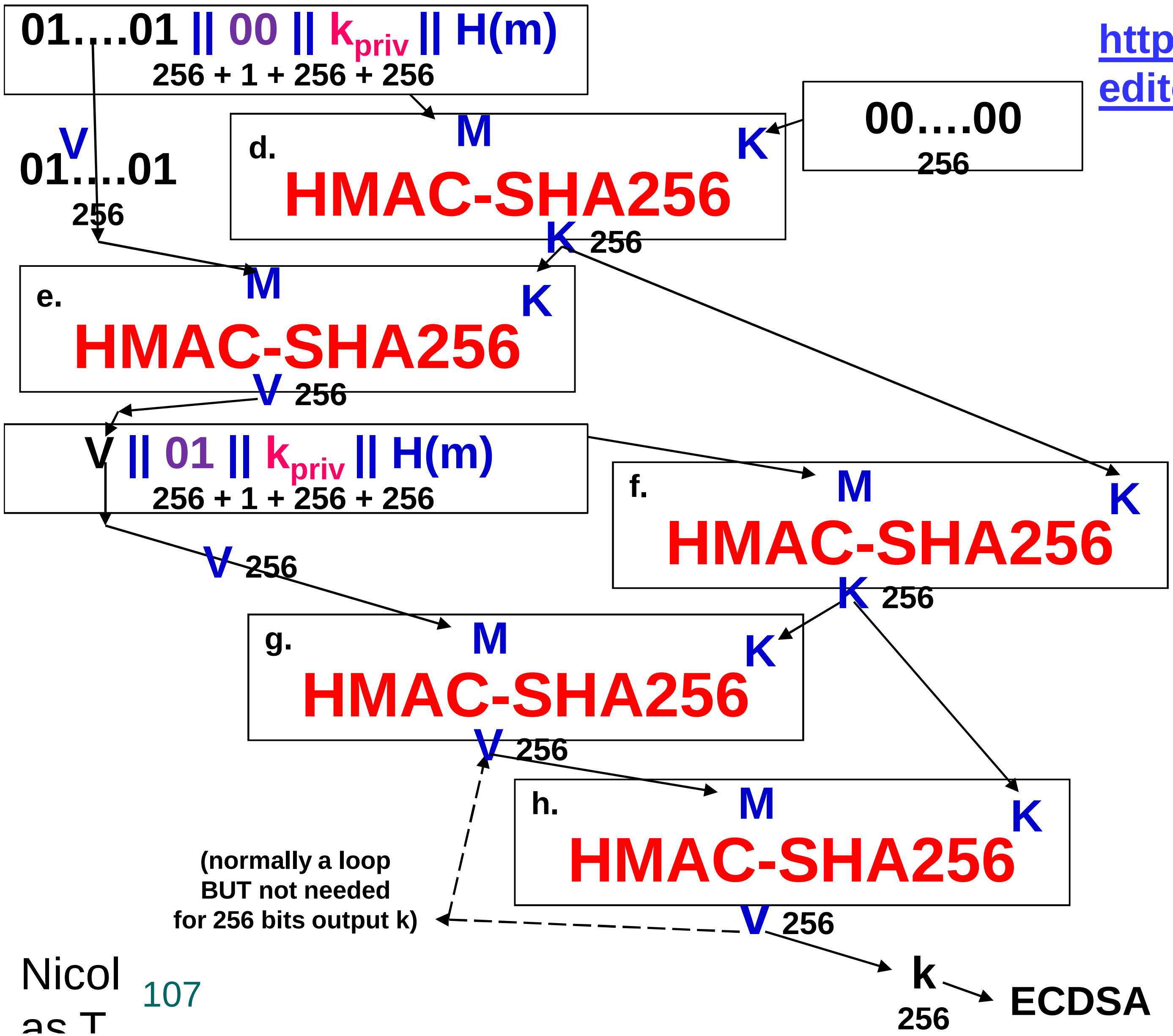
Is There a Fix?

Solution: RFC6979 [Thomas Pornin]

HOWEVER,
no existing cold storage solution
which have NOT already applied RFC6979
can claim to resist our attacks.

RFC6979 [Pornin] = 5+ applications of HMAC

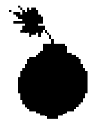
http://www.rfc-editor.org/rfc/rfc6979.txt



Which Systems Are Affected?

Solution: RFC6979 [Pornin]

- Alredy applied by
  - Electrum,Multibit, Trezor
- Yet unpatched:
  - blockchain.info – insecure,
  - BitcoinD Core – waiting for a patch to be applied,



Details:

a talk at Hack in The Box conference 15/10/2014:

http://conference.hitb.org/hitbsecconf2014kul/materials/D1T1%20-%20Filippo%20Valsorda%20-%20Exploiting%20ECDSA%20Failures%20in%20the%20Bitcoin%20Blockchain.pdf