Overview of Blockchain Security

- in Crypto we Trust -

Nicolas T. Courtois

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

UCL RESEARCH CENTRE FOR BLOCKCHAIN TECHNOLOGIES

Questions:

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

2%

Anarchy? Dark Side

- In Bitcoin many things which are BUGS are presented as FEATURES:
  - monetary policy (or the lack of one) – frequent criticism
  - problematic cryptography=
    - anonymous founder syndrome, standardized yet TOTTALLY disjoint from normal industrial cryptography, NOBUS syndrome (NSA jargon)
  - decision mechanisms (the Longest Chain Rule)
    - no reason why the same mechanism decides which blocks are valid and which transactions are valid, by far too slow, too unstable, too easy to manipulate
  - 51% attacks ARE realistic feasible and … INEXPENSIVE!
  - sudden jumps in monetary policy => genetically-programmed self-destruction of many crypto currencies

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

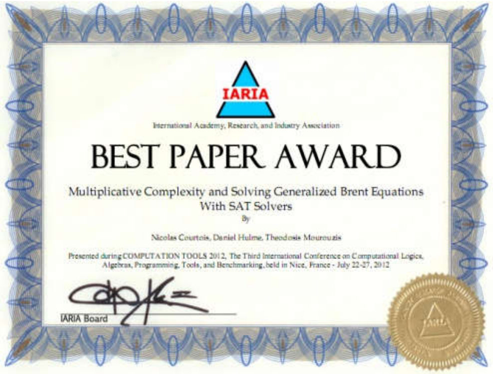
Dangers of Open Source

- 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 [...]

Cf. Vivian A. Maese: Divining the Regulatory Future of Illegitimate Cryptocurrencies, In Wall Street Lawyer, Vol. 18 Issue 5, May 2014.

Dr. Nicolas T. Courtois

1. cryptologist and codebreaker



IARIA

International Academy, Research, and Industry Association

BEST PAPER AWARD

Multiplicative Complexity and Solving Generalized Brent Equations
With SAT Solvers

By

Nicolas Courtois, Daniel Hulme, Theodosis Mourouzis

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

IARIA Board

NewScientist

The global science and technology weekly | 7 June 2003

NEW! US JOBS SECTION

MEGAWATER

The biggest engineering folly of all time?

JOHN BARROW

How our world could be just a computer simulation

CIPHER CRISIS

UNIVERSITY CIPHER CHAMPION

March 2013

Cyber Security Challenge UK

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

Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

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

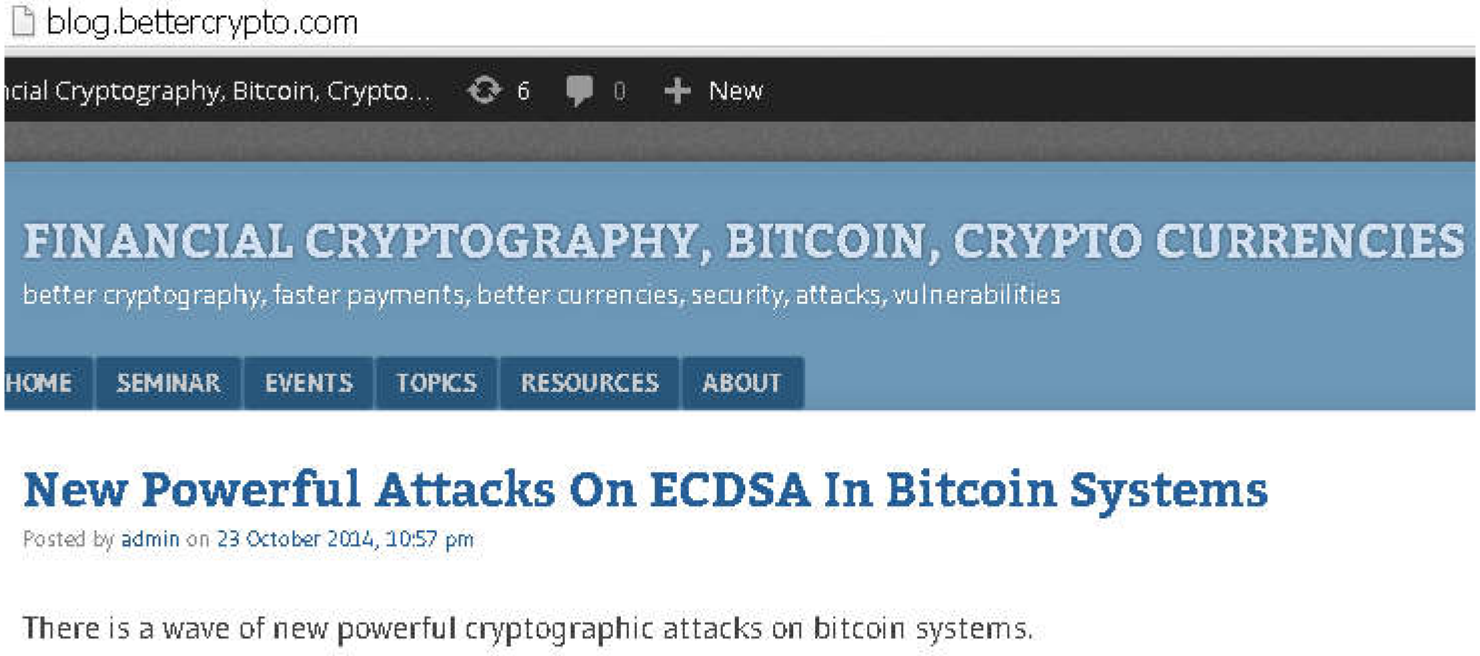
-Nicolas T. Courtois, Pinar Emirdag and Daniel A. Nagy: Could Bitcoin Transactions Be 100x Faster? In proceedings of SECRYPT 2014, 28-30 August 2014, Vienna, Austria.

-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

My Blog and Bitcoin Events@UCL

blog.bettercrypto.com



blog.bettercrypto.com

FINANCIAL CRYPTOGRAPHY, BITCOIN, CRYPTO CURRENCIES

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

New Powerful Attacks On ECDSA In Bitcoin Systems

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

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

“Cryptographer’s Dream”

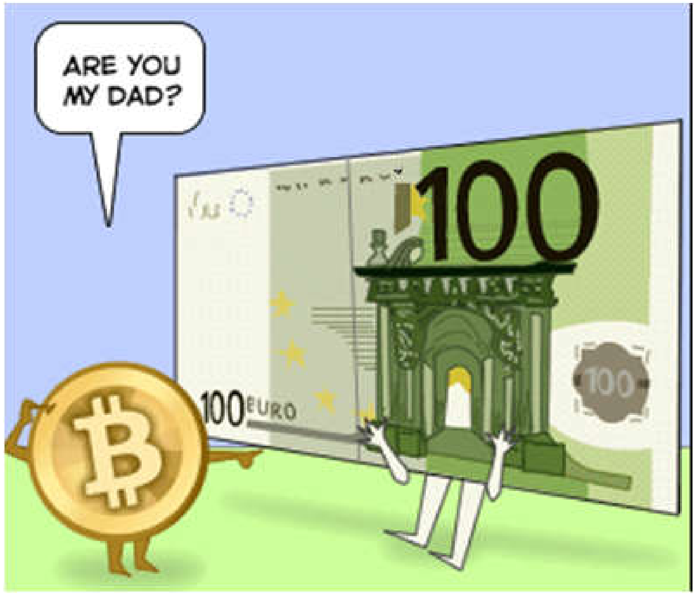
- Building “trust-less” systems and a “trust-less” society.

“Cryptographer’s Dream”

- Building “trust-less” systems and a “trust-less” society.
- How?
- Crypto “protocols” with several parties who do not know each other in advance and
  WITHOUT any trusted authorities:
  lawyers, notaries, CAs, bankers, accountants, auditors, policemen, law makers, government officials, etc…

  – Modern cryptography makes such things possible…

Bitcoin



Bitcoin

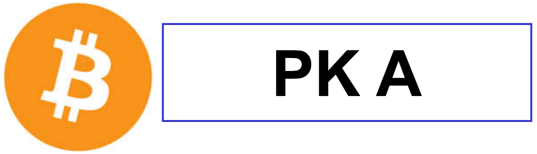
Based on cryptography and network effects.

Private money.

Bitcoin

Bitcoins are cryptographic money

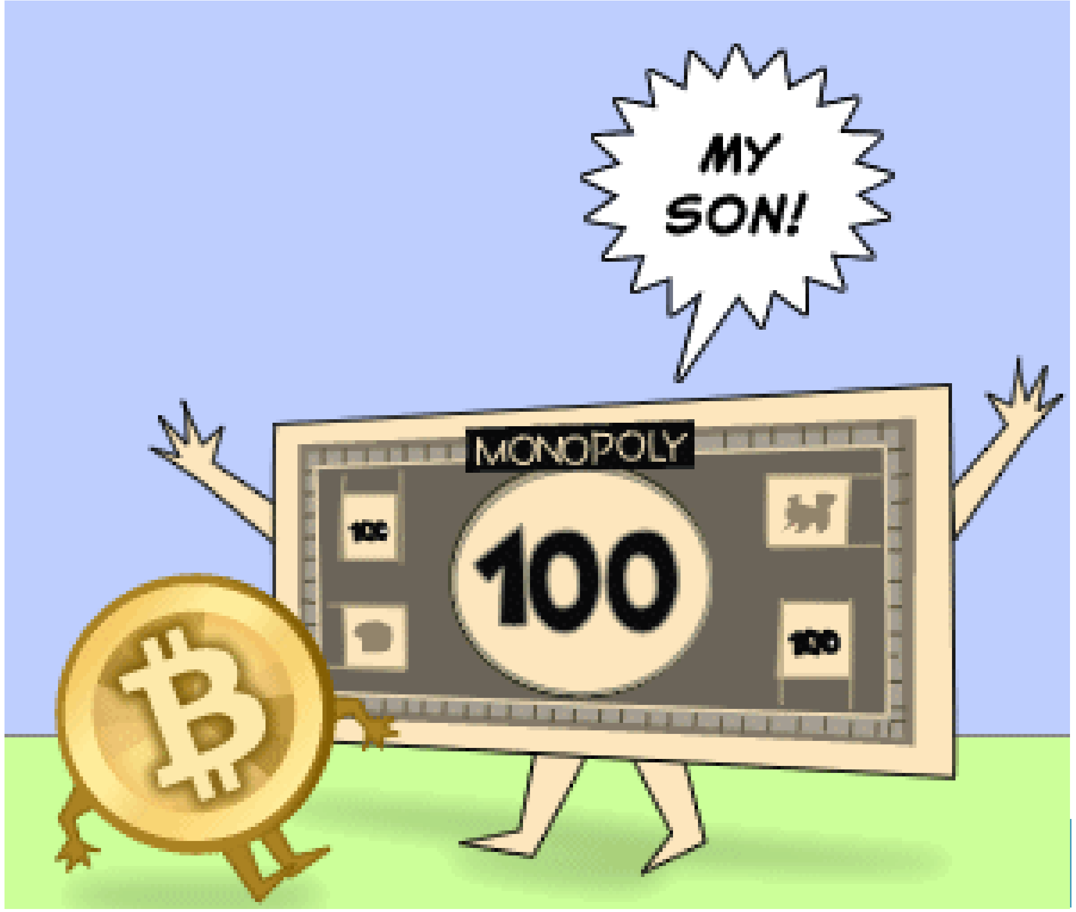
- public ledger:
  - history shows how many bitcoins each user has
  - one user - many accounts = pseudonyms



PK A

Are They Crazy?

Anything can be “money”
if sufficiently many people accept it…



A question of:

- popularity

replaces the government-imposed standardization

- trust

<= distributed computer system
acting on self-interest
NO NEED TO TRUST ANYONE

E-Cash[Chaum’83] and Bitcoin[Nakamoto‘08]

New Coins

initially X coins 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)
- do a difficult computation => you have earned 25 bitcoins
- works like a lottery (1 winner/10 minutes)

PK A

public ledger says H(PK A) has 1 BTC

New Coins

initially X coins 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)
- do a difficult computation => you have earned 25 bitcoins
- works like a lottery (1 winner/10 minutes)

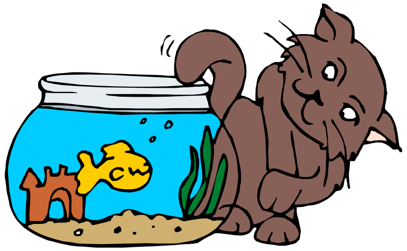
PK A

**public ledger says
H(PK A) has 1 BTC**

*alternative solution:
bank/trusted authority/mintette can attribute coins initially

Authorizing Transfer of Coins

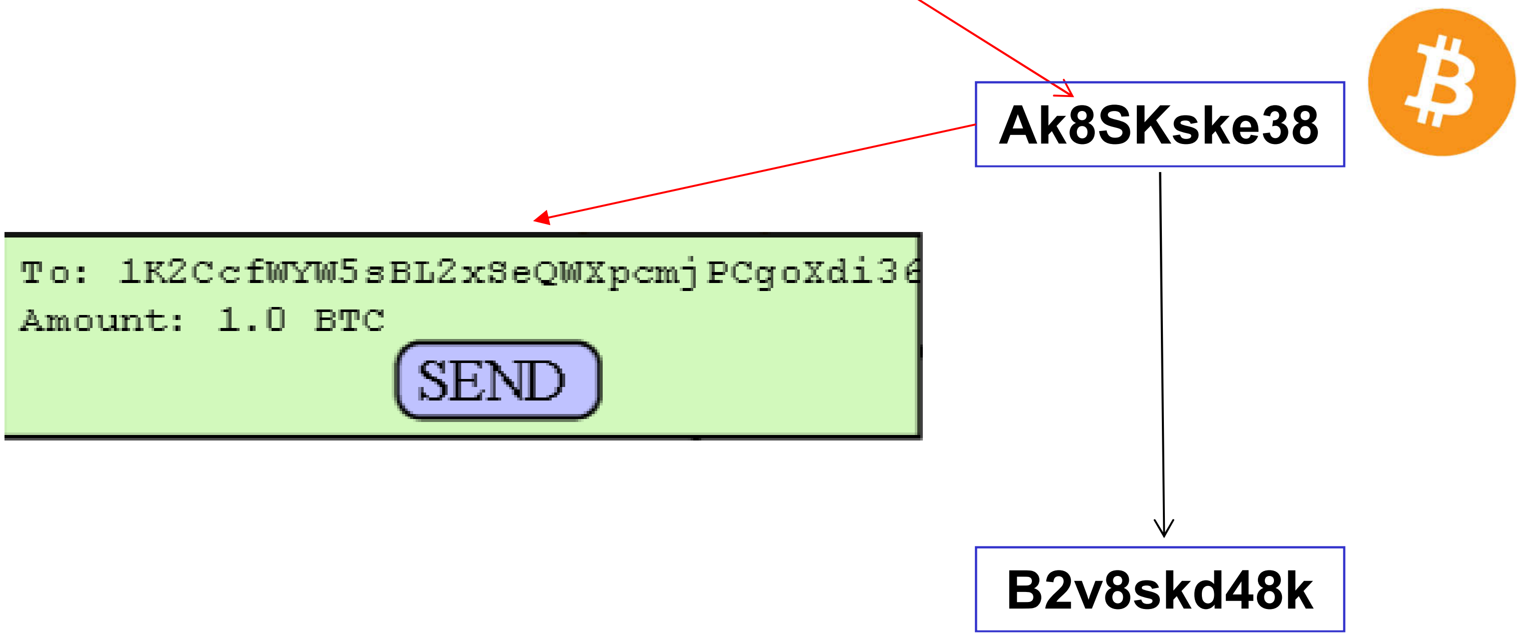
- you have a private key => you have the money (right to transfer)
  - money stored on PCs or mobile phones?



  - better solution: smart card

Bitcoins

- user has the right to transfer his bitcoins to any other user
  - user are known by their pseudonyms, H(PKeys)
  - one person => many pseudonyms / accounts

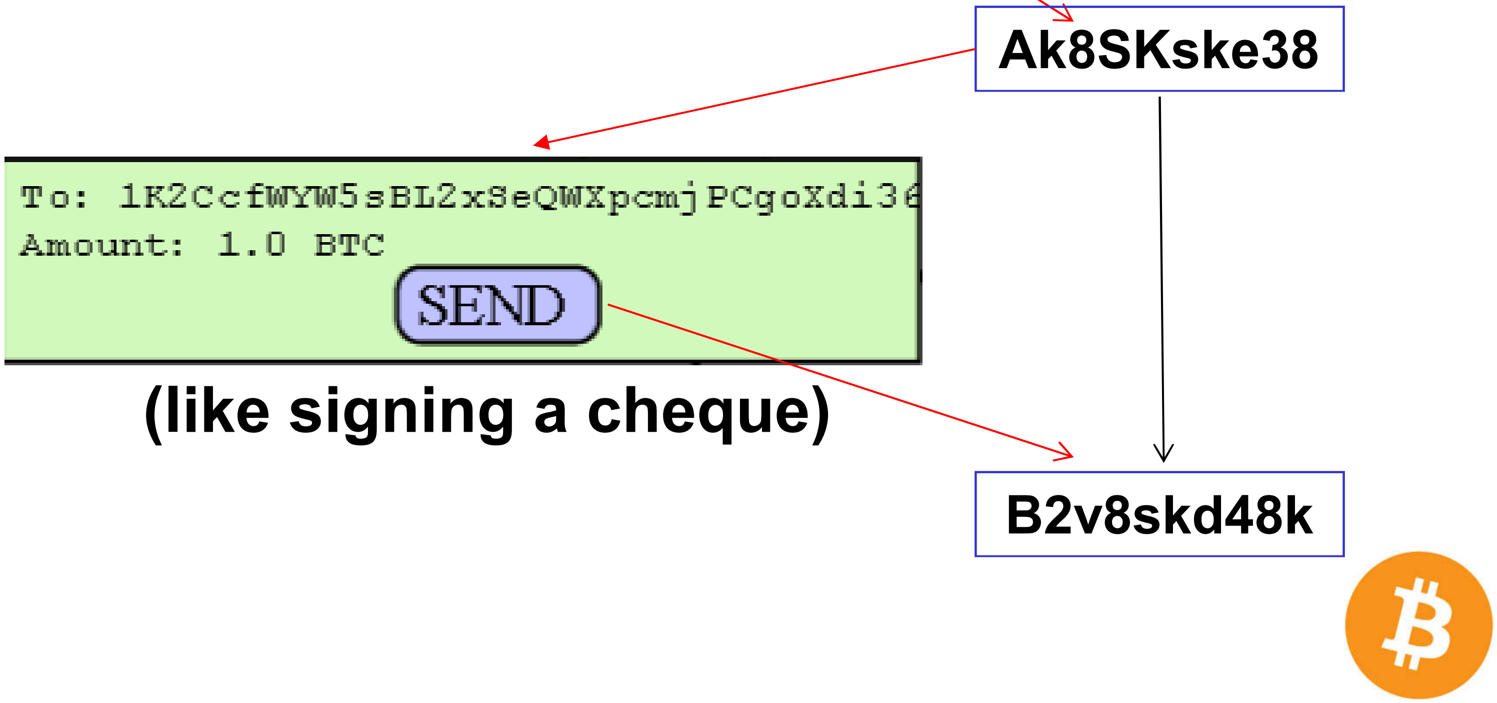


To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36

Amount: 1.0 BTC

Bitcoins

- user has the right to transfer his bitcoins to any other user
  - user are known by their pseudonyms, H(PKeys)
  - one person => many pseudonyms / accounts



To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36

Amount: 1.0 BTC

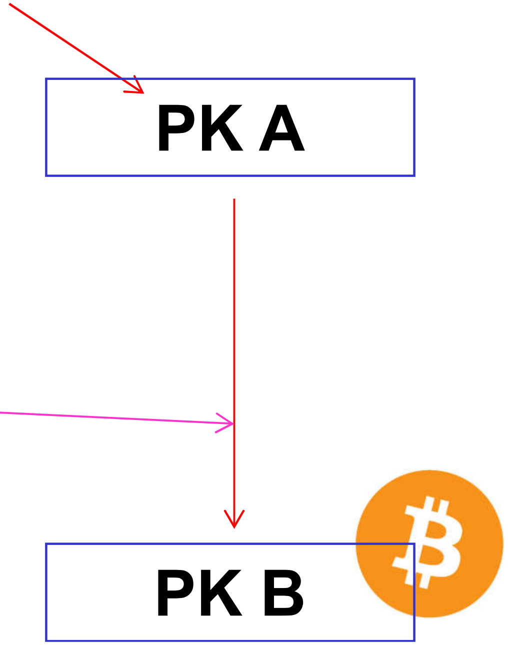
(like signing a cheque)

Transfer of Coins

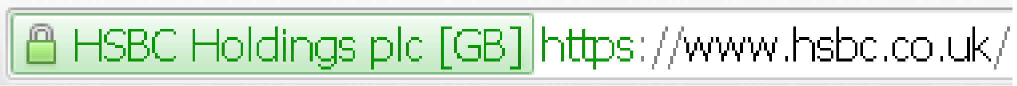
- hard work => public key A

- money transfer PK A => PK B

digital signature authorizes the transfer



Digital Signatures



HSBC Holdings plc [GB] https://www.hsbc.co.uk/

Digital Signatures

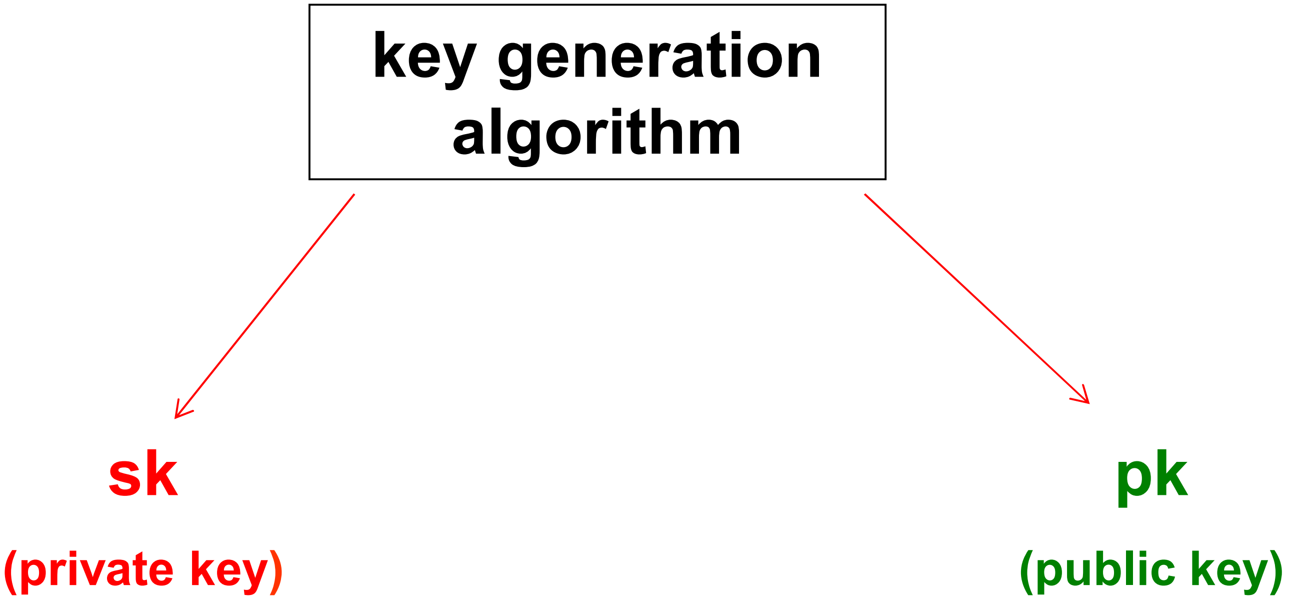
- Origin Tx(s)
- Amount(s)
- New Owner(s)

Signature

Digital Signatures

Idea: cryptographic solution

3 algorithms…



key generation algorithm

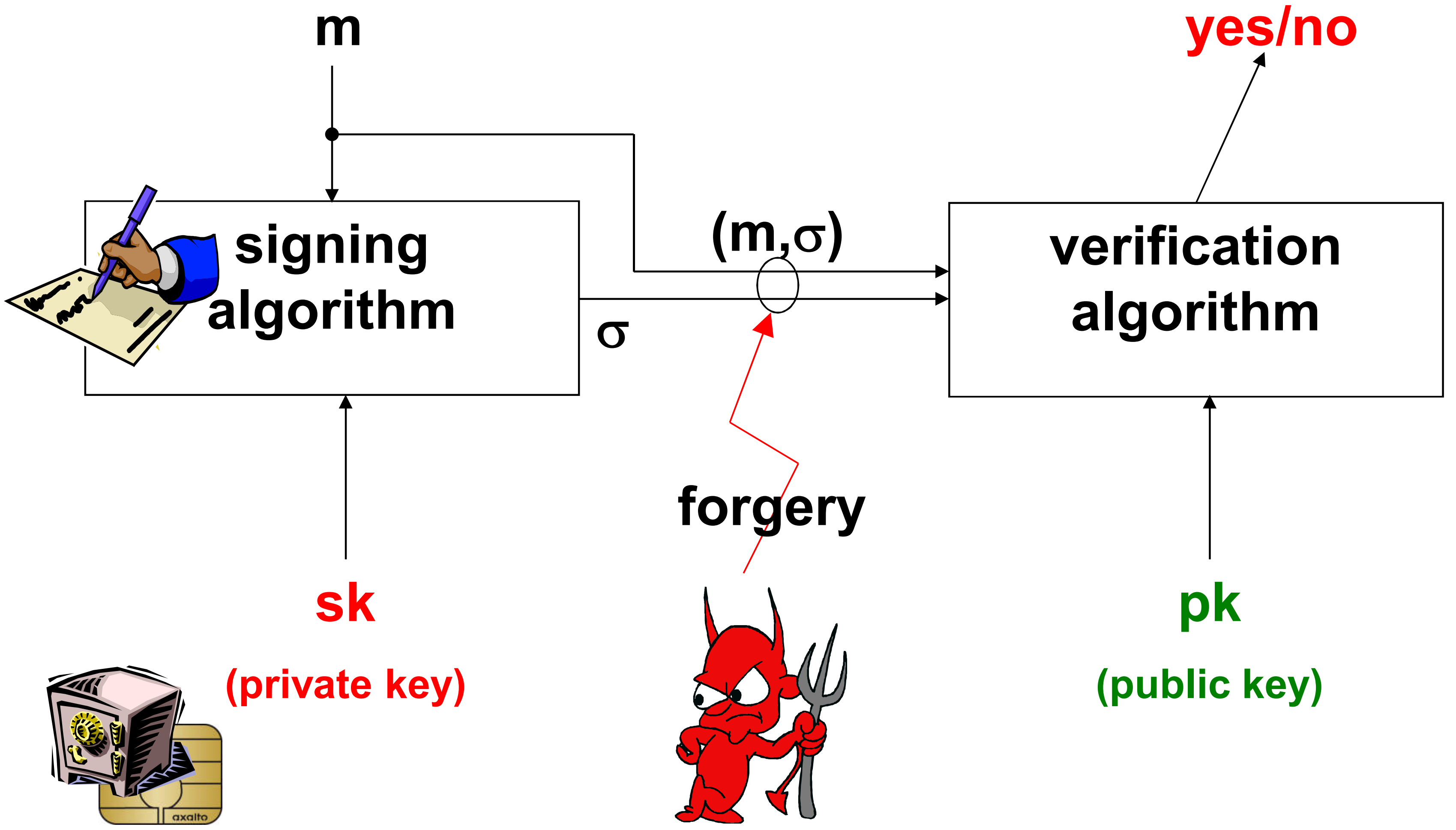
sk

(private key)

pk

(public key)

Digital Signature



m

yes/no

signing algorithm

(m,σ)

verification algorithm

σ

forgery

sk

(private key)

pk

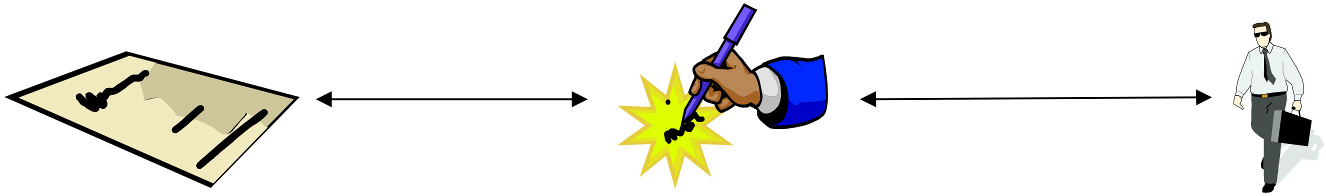
(public key)

2x Link

EU Directive 1999 => national laws…

e.g. UK Electronic Communications Act 2000

France: *article 1316-4 du code civil*



Signatures - Requirements

1. Authenticity – guarantees the document signed by…
2. Non-repudiation

   = Imputability
3. **BONUS:**

   Public verify-ability -

   anyone can verify!

0. Completeness – **honest signer always accepted**

1. Soundness – **dishonest signer always rejected**

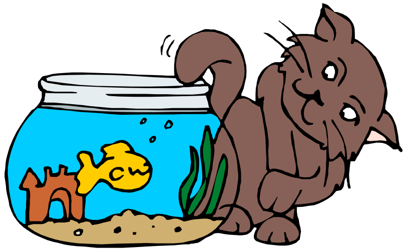
Secure Digital Signature

[Goldwasser-Micali-Rivest 1988]

EUF - CMA (Existential Unforgeability under CMA)

1. Adversarial Goal.

   Find any new pair (m,σ) (new m)!

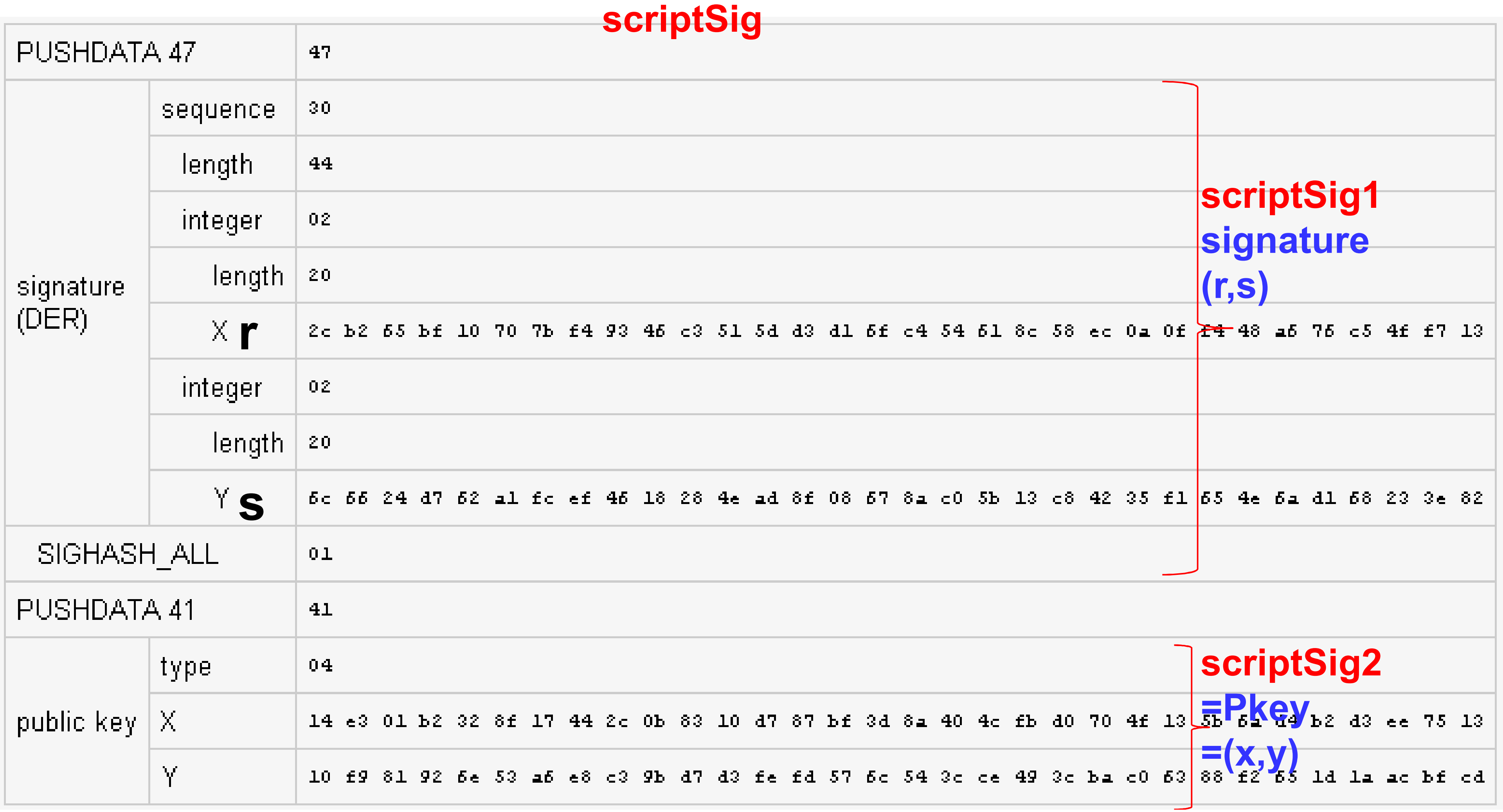


2. Resources of the Adversary:
   Any Probabilistic Turing Machine doing 2^{100} computations.

3. Access / Attack:
   May sign any message except one (target).
   (Adaptively Chosen Message Attacks).

Typical Signature ∈ Tx

sign+PKey



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)

Trust Less!

Digital Signatures ENABLE
these TRUSTLESS systems!

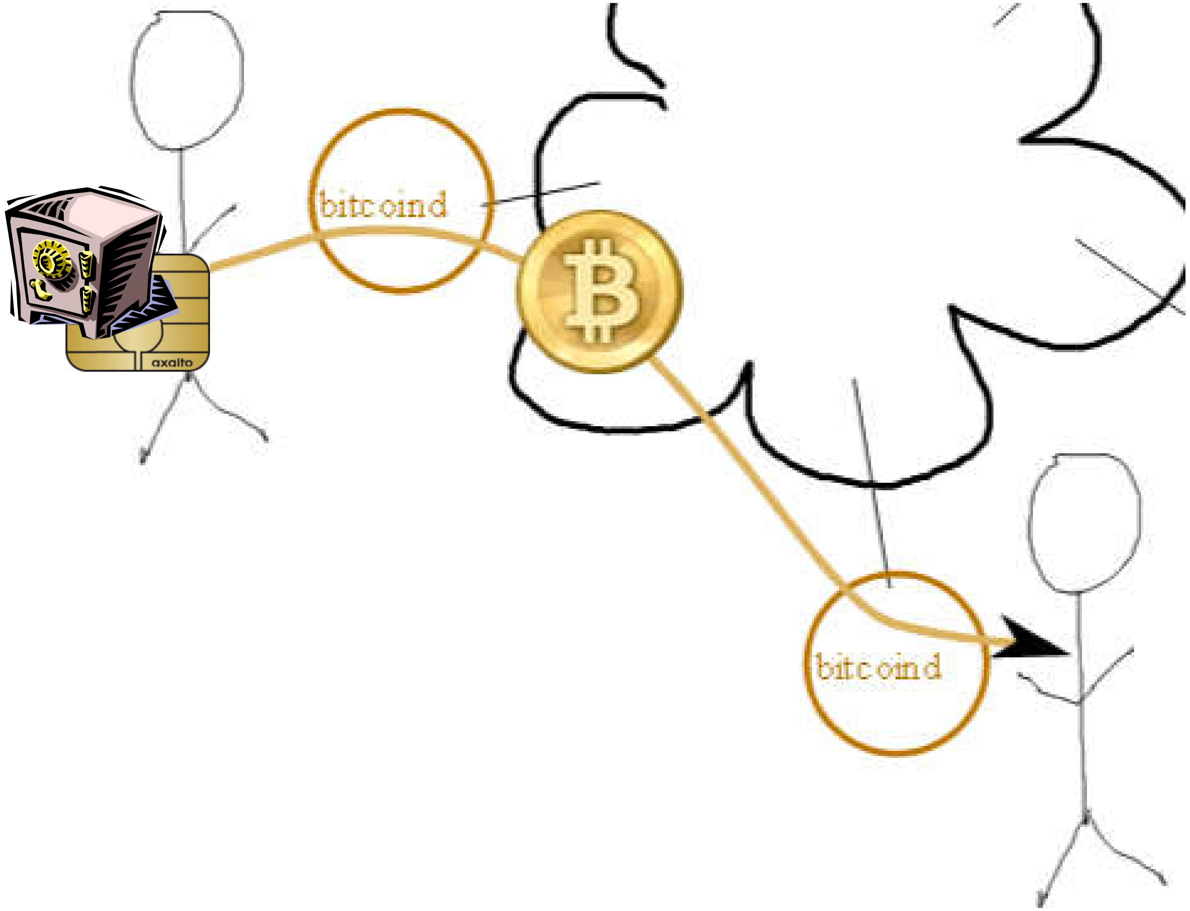
Example: My bank card signs a transaction with RSA, the bank does NOT know the private key,
ONLY the public key.

⇒We do NO LONGER need to trust the bank.

⇒The banker cannot forge transactions done with my card!

Bank Card => Bitcoin

Bitcoin is a "private" / decentralized descendant of the French bank card



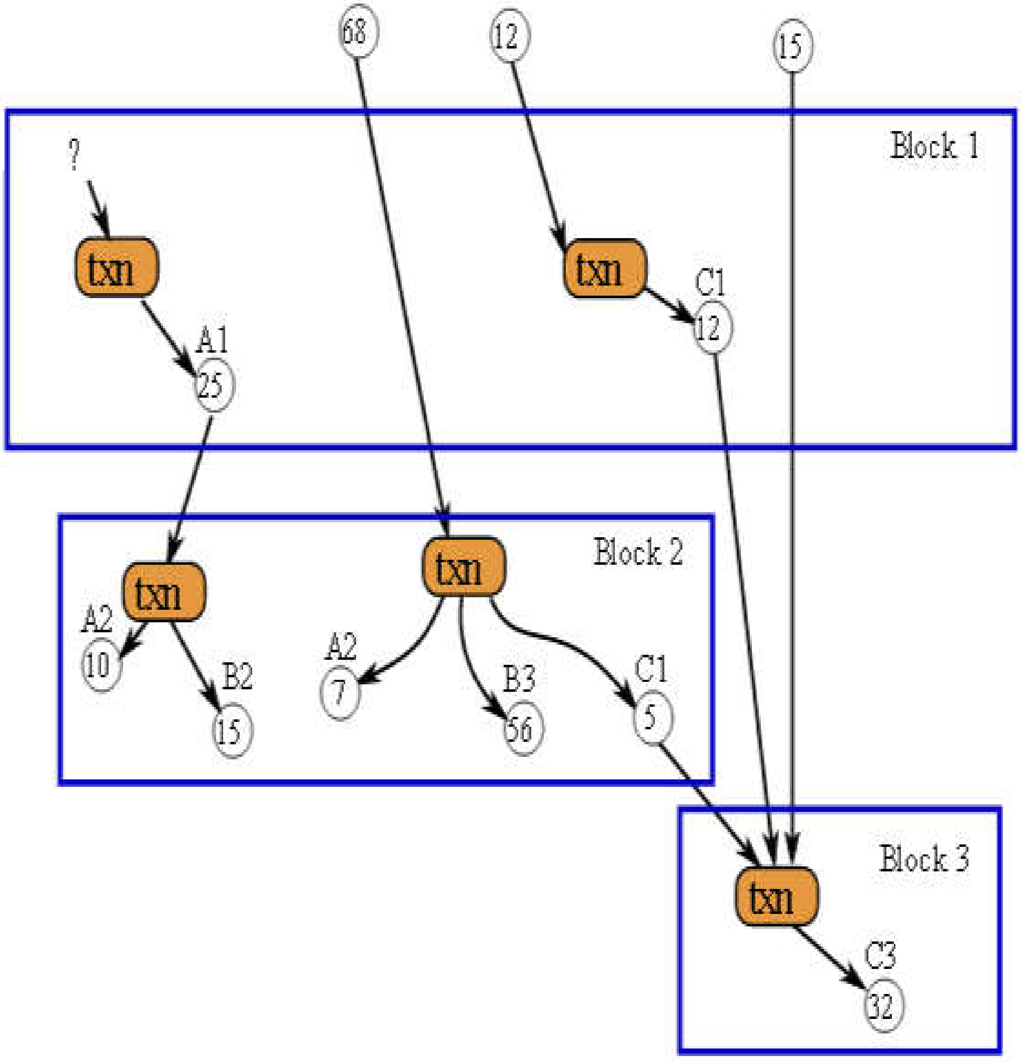
Block Chain

Def:

Public transaction database
or a ledger.

Every transaction
since ever is public.

Each block contains a
Proof Of Work (POW)
(blocks are hard to make)



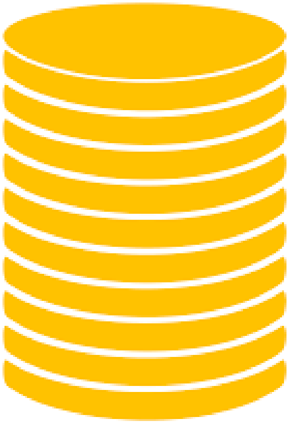
Multiple Confirmations

=>each new block confirms
ALL previous events

<u>Security:</u>

we do NOT need to assume
that ALL people are honest.

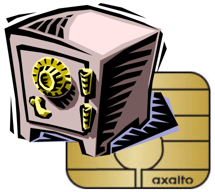
- evidence piles up
- with time it becomes too costly to cheat



Bitcoin Network

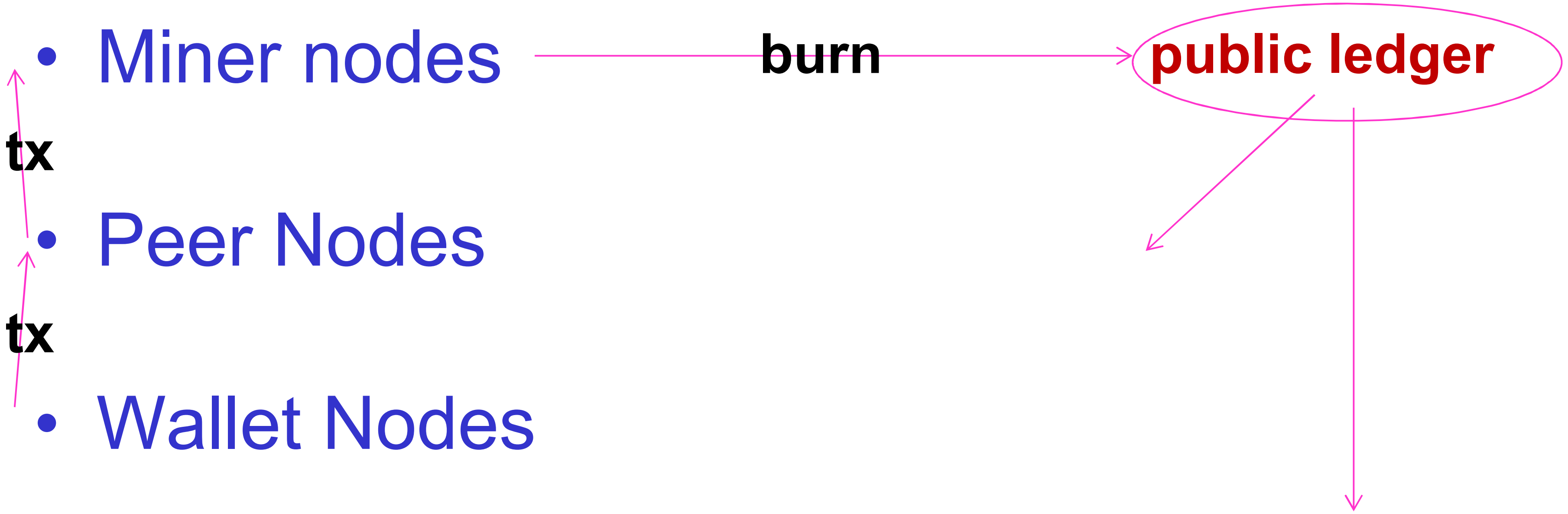
Three sorts of entities:

- Miner nodes – 50K
  - – Hashing with public keys
- Peer Nodes – 5K
  - – Relay and store transactions and blocks
- Wallet Nodes – 5.5M, 0.25M active
  - – store private keys



=>can spend the money

Tx LifeCycle



- Miner nodes

burn

public ledger

tx

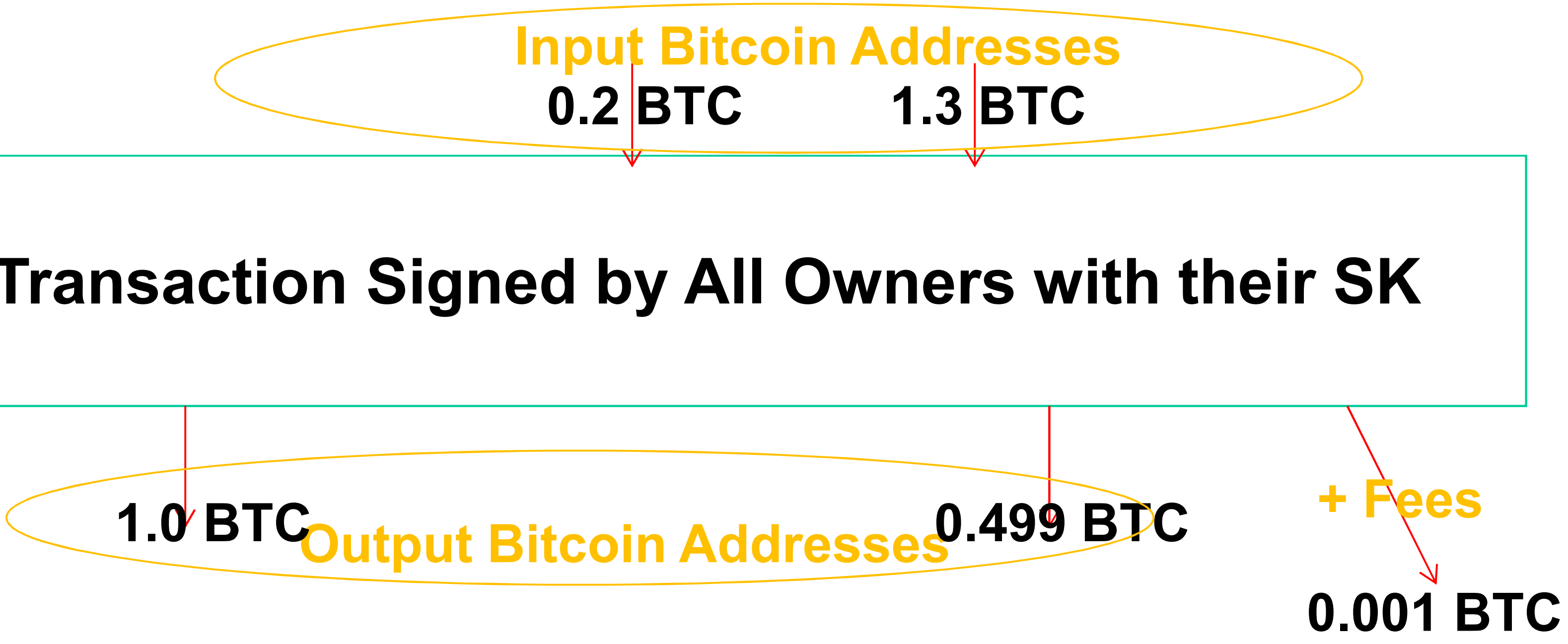
- Peer Nodes

tx

- Wallet Nodes

Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



Input Bitcoin Addresses

0.2 BTC 1.3 BTC

Transaction Signed by All Owners with their SK

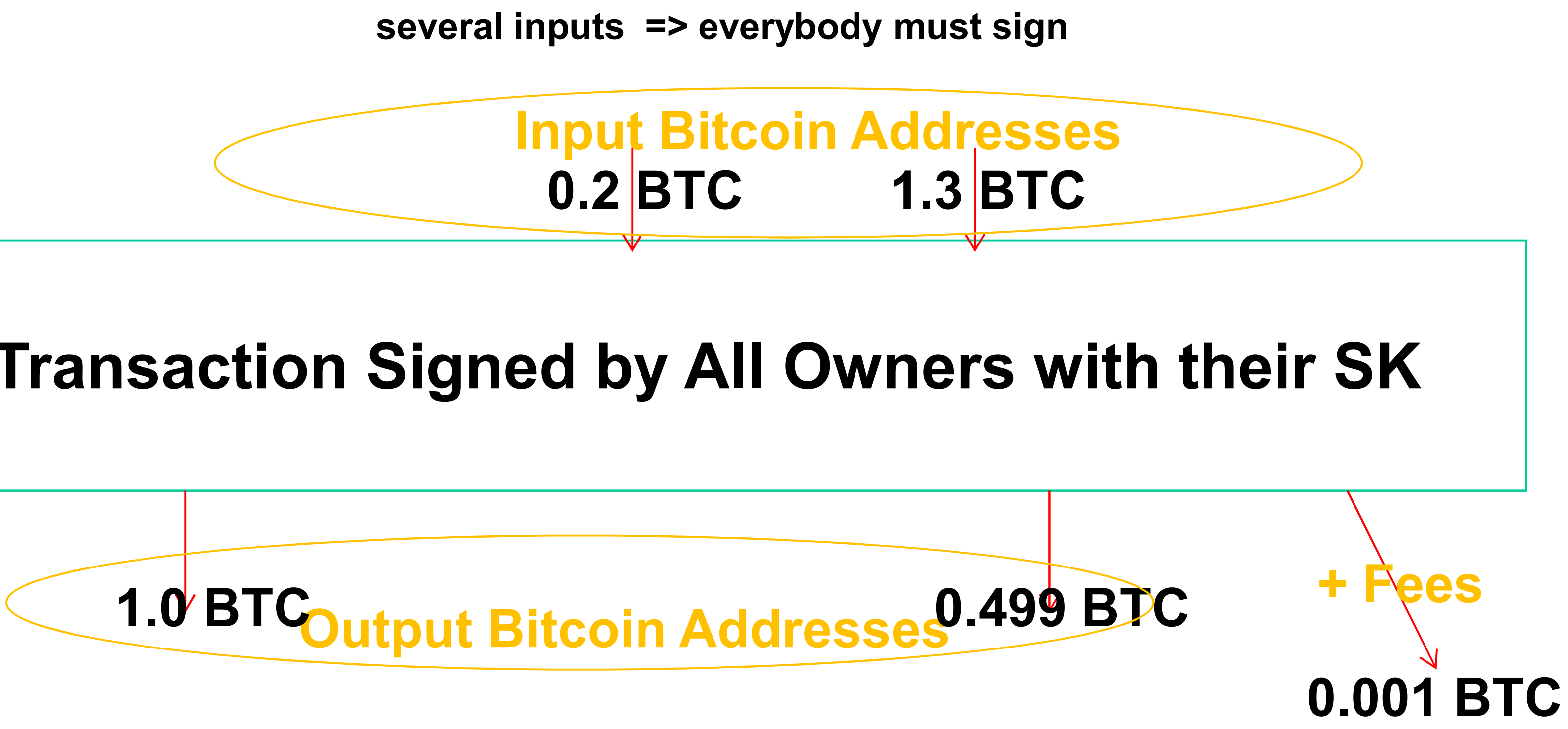
1.0 BTC Output Bitcoin Addresses 0.499 BTC

+ Fees

0.001 BTC

Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



several inputs => everybody must sign

Input Bitcoin Addresses

0.2 BTC 1.3 BTC

Transaction Signed by All Owners with their SK

1.0 BTC Output Bitcoin Addresses 0.499 BTC

+ Fees

0.001 BTC

Multi-Signature Addresses

MultiSig = Addresses Starting with 3

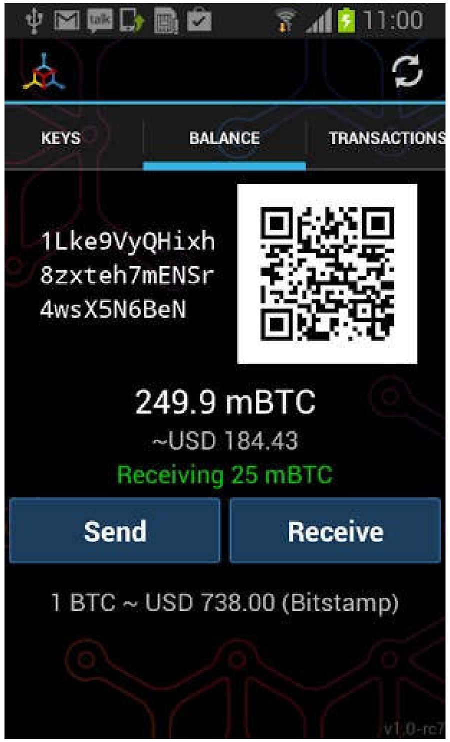
Bitcoin can require simultaneously several private keys, in order to transfer the money.

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

Is Bitcoin Secure?

Satoshi claimed it is…

Wallets



1Lke9VyQHixh
8zxteh7mENSr
4wsX5N6BeN

249.9 mBTC

~USD 184.43

Receiving 25 mBTC

1 BTC ~ USD 738.00 (Bitstamp)

Bottom Line

Main Functionality:

-Private Key Generation

-Export public key

-ECDSA sign

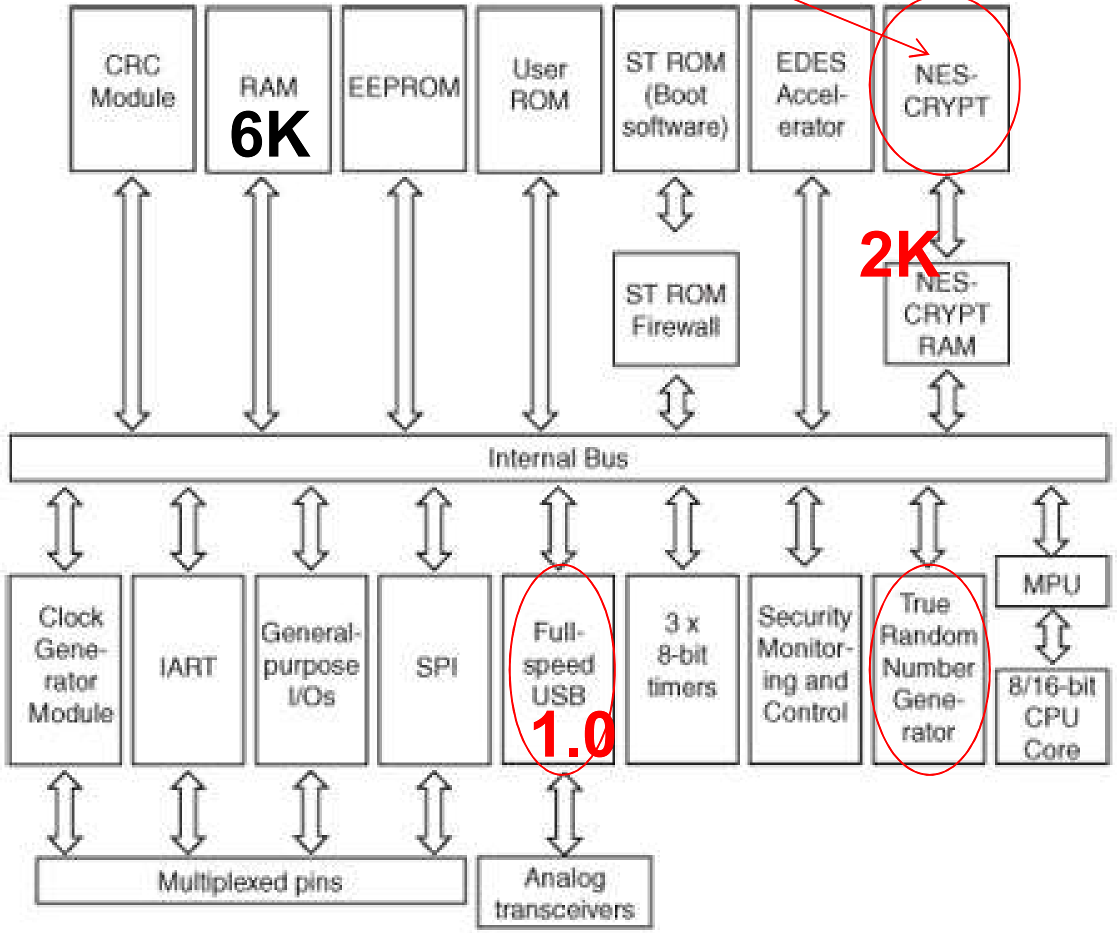
Ledger

ledgerwallet.com

Banking card platform ST23YT66

NESCRYPT crypto-processor for PK crypto

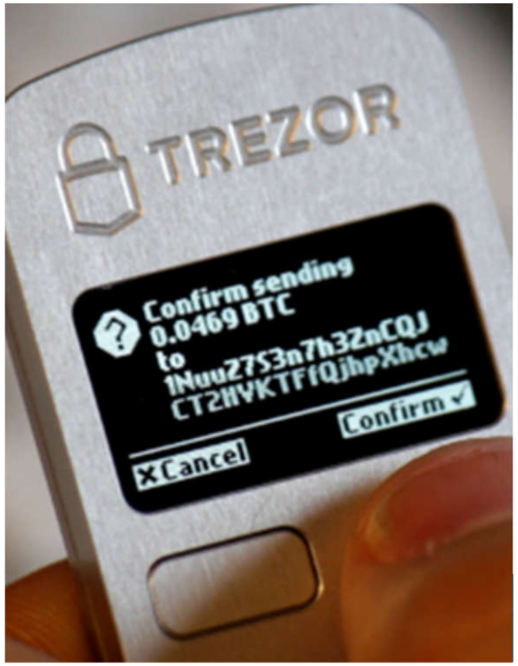
- 900 ms for 1 ECDSA signature
- 900 ms for key gen
- encrypts private keys on the card ('content' key) 3DES CBC
    - content key can be protected with "a GlobalPlatform Secure Channel" authentication mechanism



Ledger Nano S [2016] vs. Trezor [older]

+ display: know to whom you send the money!

+buttons to enter PIN/approve.



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).

Least Common Mechanism

Violated in Bitcoin with:

- Open SSL and other standard libraries with massive amounts of code which is not useful at all for bitcoin
- when using TOR
- with current consensus rules!!!!

Least Common Mechanism

Violated in Bitcoin:

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

2 July 2014.

At minute 02.55: Dr. Nicolas Courtois of UCL:

"…One of the fundamental mistakes of bitcoin is that they use 'the Longest Chain Rule' to decide simultaneously
which block gets accepted and
which transactions get accepted,
[…] a big mistake."

Open Design Principle

[Saltzer and Schroeder 1975]

Open Design ≠ Open Source

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

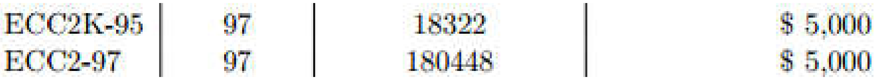
NATIONAL SECURITY AGENCY

Citation

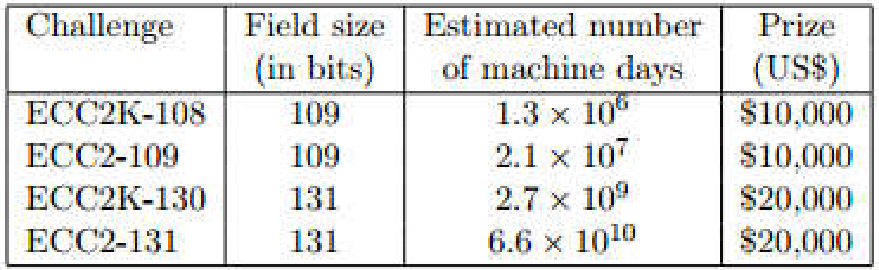
Bitcoin is:

- Wild West of our time [Anderson-Rosenberg]

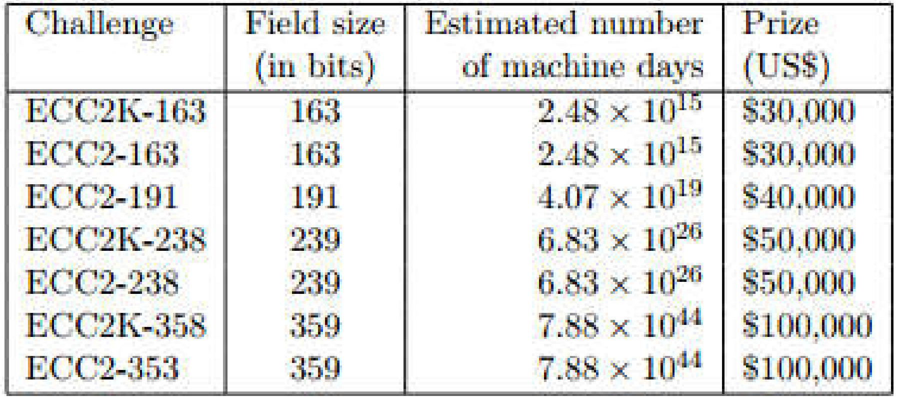
ECC - Certicom Challenges [1997, revised 2009]



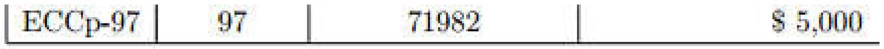
ECC2K-95	97	18322	$ 5,000
ECC2-97	97	180448	$ 5,000



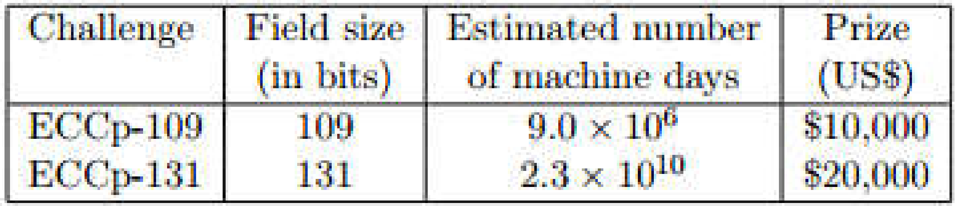
Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECC2K-108	109	1.3×10^6	$10,000
ECC2-109	109	2.1×10^7	$10,000
ECC2K-130	131	2.7×10^9	$20,000
ECC2-131	131	6.6×10^{10}	$20,000



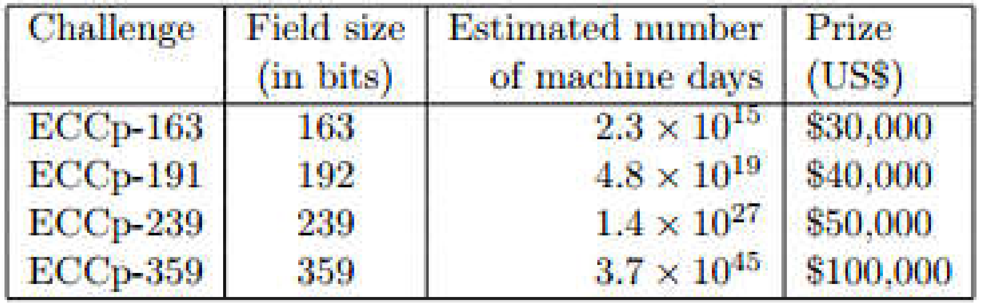
Challenge	Field size (in bits)	Estimated number of machine days	Prize (US$)
ECC2K-163	163	2.48×10^{15}	$30,000
ECC2-163	163	2.48×10^{15}	$30,000
ECC2-191	191	4.07×10^{19}	$40,000
ECC2K-238	239	6.83×10^{26}	$50,000
ECC2-238	239	6.83×10^{26}	$50,000
ECC2K-358	359	7.88×10^{44}	$100,000
ECC2-353	359	7.88×10^{44}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

Official Bitcoin Wiki

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

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

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

Bitcoin has a sound basis in well understood cryptography.

Official Bitcoin Wiki

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

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

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

Bitcoin has a sound basis in well understood cryptography.

Well…actually it has major bug in it.

⇒ Major security scandal in the making?

⇒ Expect a lawsuit??? for

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

Blame Satoshi ☺

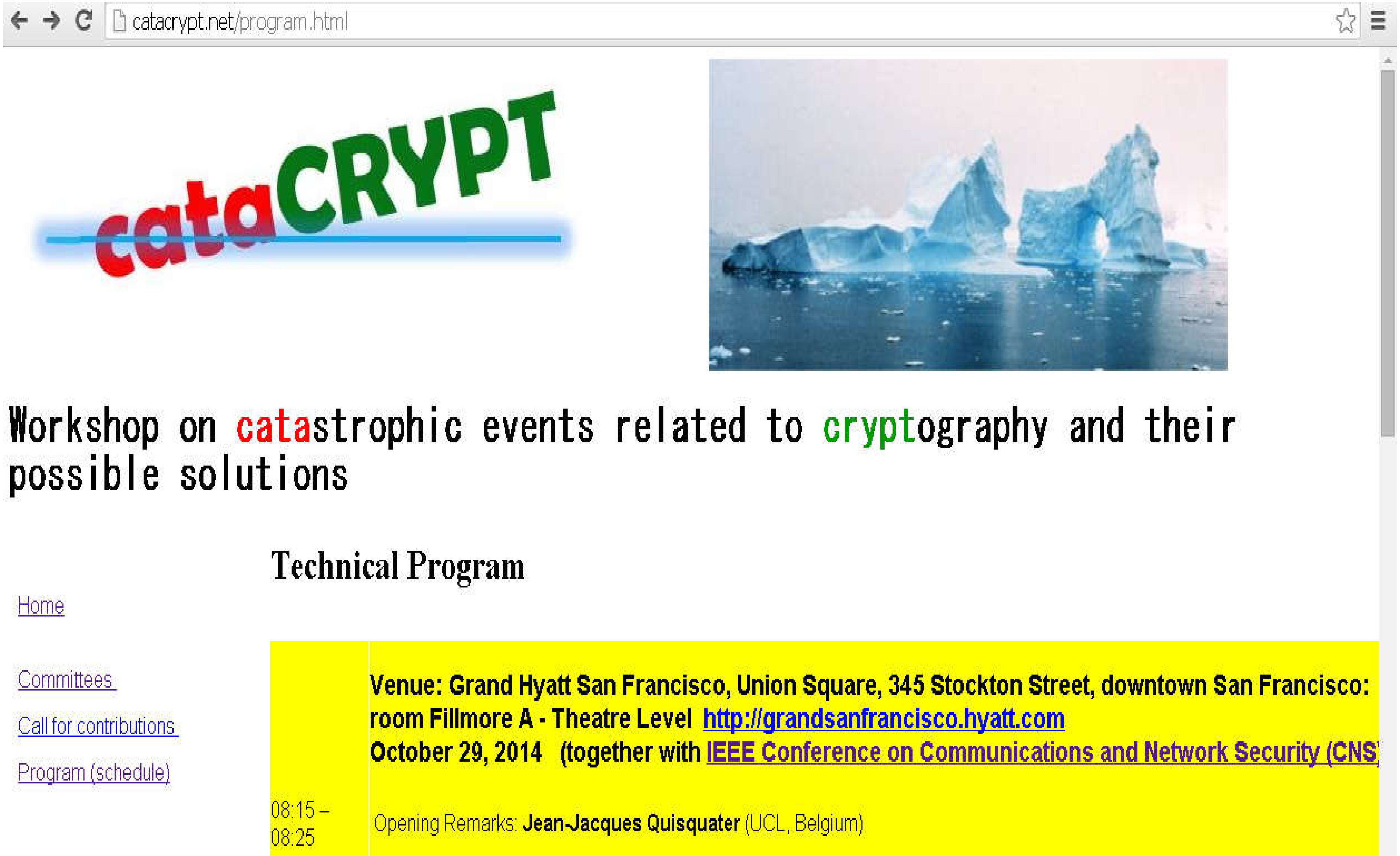
Officially Not Recommended

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

”I am surprised to see anybody use secp256k1”

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

What If? CataCrypt Conference



Workshop on catastrophic events related to cryptography and their possible solutions

Technical Program

Home

Committees

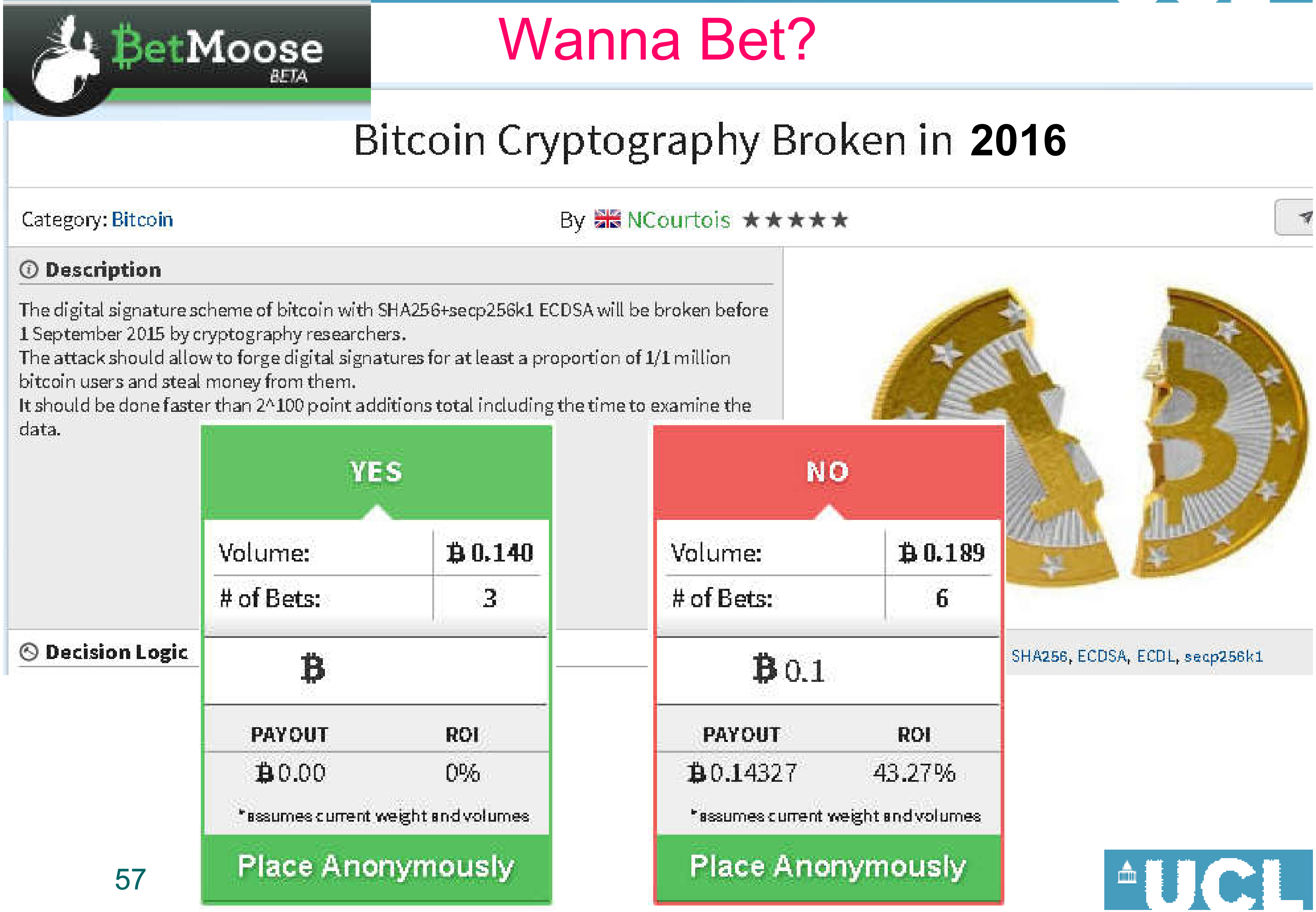
Call for contributions

Program (schedule)

Venue: Grand Hyatt San Francisco, Union Square, 345 Stockton Street, downtown San Francisco: room Fillmore A - Theatre Level http://grandsanfrancisco.hyatt.com
October 29, 2014 (together with IEEE Conference on Communications and Network Security (CNS)

08:15 – 08:25 Opening Remarks: **Jean-Jacques Quisquater** (UCL, Belgium)

Wanna Bet?



BetMoose BETA

Bitcoin Cryptography Broken in 2016

Category: Bitcoin

By NCourtois ★★★★★

Description

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

Decision Logic

SHA256, ECDSA, ECDL, secp256k1

YES

Volume:	฿ 0.140
# of Bets:	3

฿

PAYOUT	ROI
฿0.00	0%

*assumes current weight and volumes

Place Anonymously

NO

Volume:	฿ 0.189
# of Bets:	6

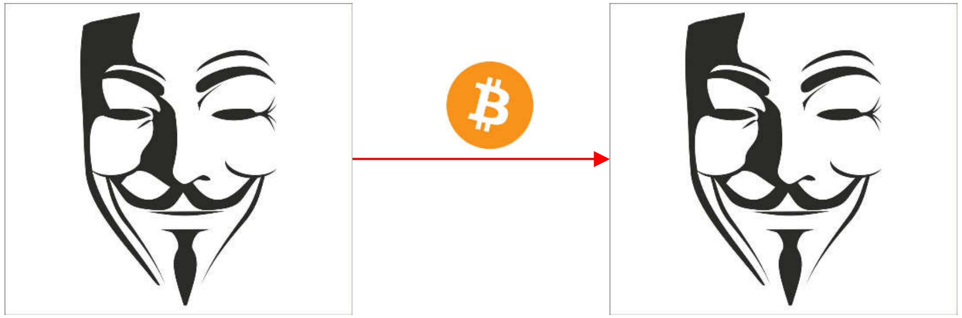
฿ 0.1

PAYOUT	ROI
฿0.14327	43.27%

*assumes current weight and volumes

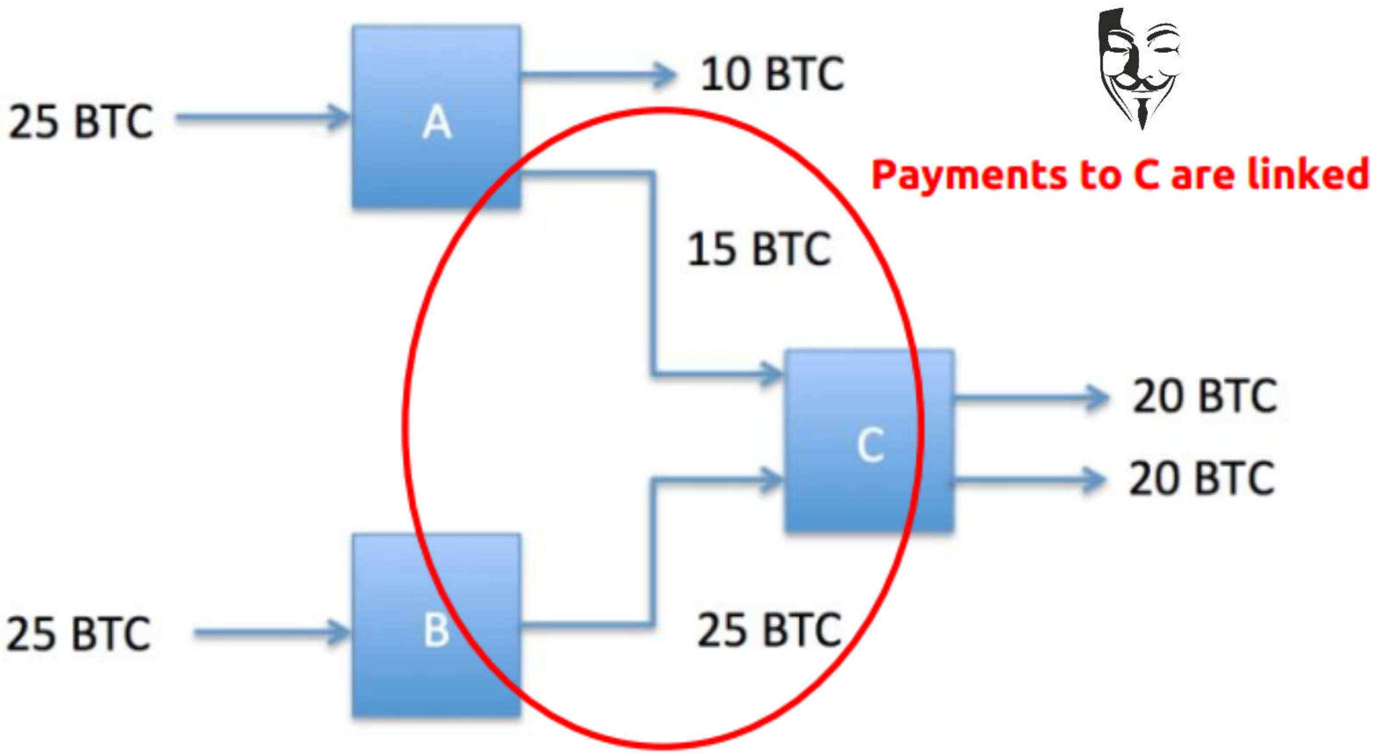
Place Anonymously

anonymous payments



not only about Monero
potentially also for bitcoin (permission-less)

Bitcoin and Linakability



Payments to C are linked

Q: Does Monero remove this????

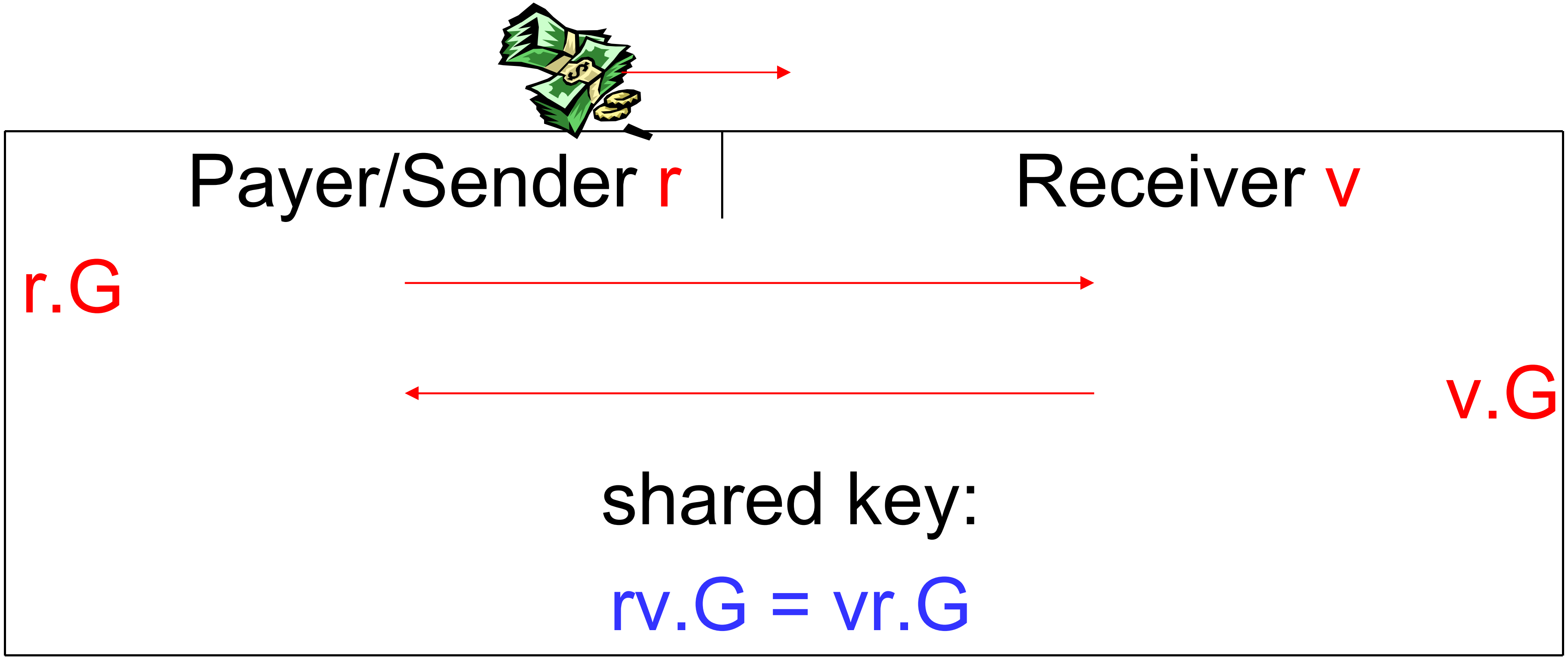
Stealth Address = “Invisible” Recipient

- user=ByteCoin [Bitccoin forum]., also attributed to Peter Todd

A Method to protect the recipient
[nobody knows I sent money to this recipient]

BTW. it is largely “permission-less”…

Stealth Address in Monero



Payer/Sender r

Receiver v

r.G

v.G

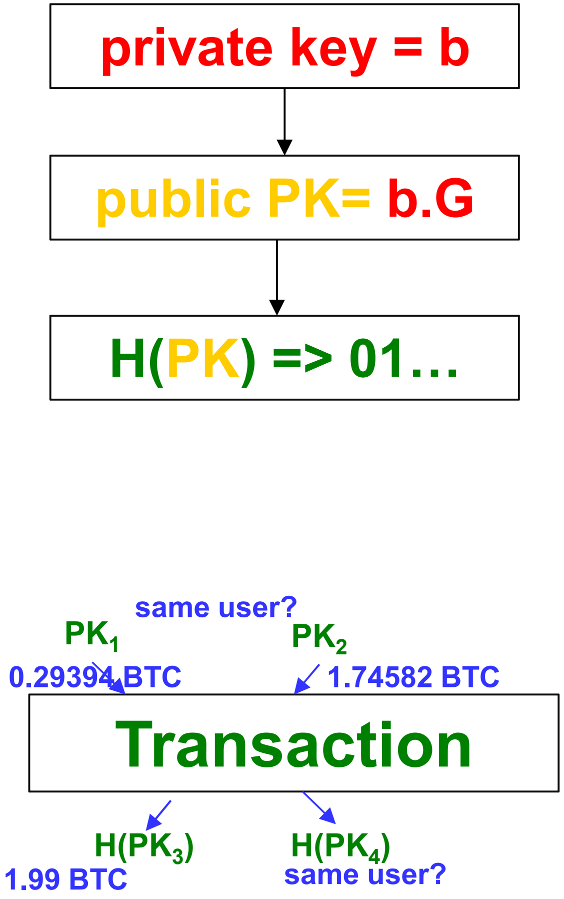
shared key:

rv.G = vr.G

Sender: S=r.(v.G). Send bitcoins to E=H(S).G+b.G.

Receiver: H(S)=H(v.(r.G)). Private key e=H(S)+b!!!

**Bitcoin vs. Monero



private key = b

public PK= b.G

H(PK) => 01…

same user?

PK_1

PK_2

0.29394 BTC

1.74582 BTC

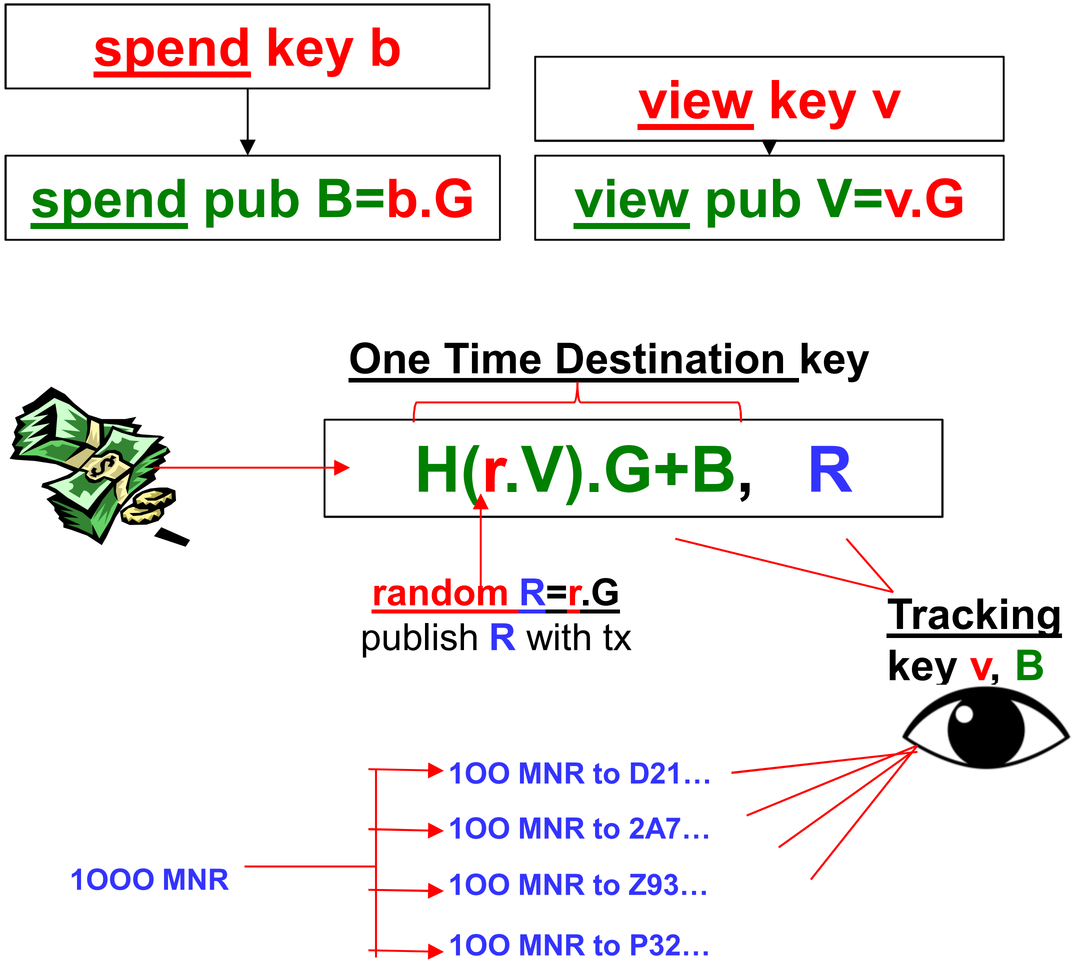
Transaction

$H(PK_3)$

1.99 BTC

$H(PK_4)$

same user?



spend key b

spend pub B=b.G

view key v

view pub V=v.G

One Time Destination key

H(r.V).G+B, R

random R=r.G

publish R with tx

Tracking

key v, B

1OOO MNR

1OO MNR to D21…

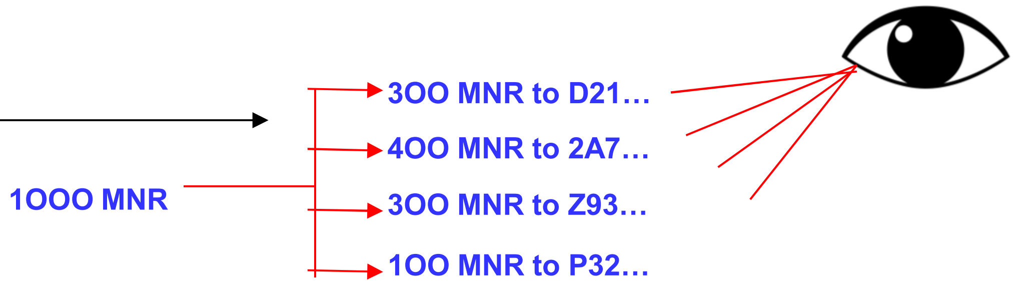
1OO MNR to 2A7…

1OO MNR to Z93…

1OO MNR to P32…

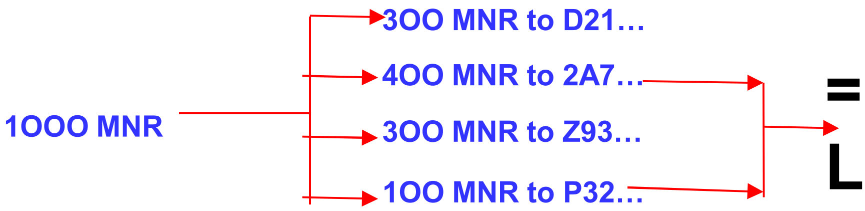
Privacy – Good?

At this moment: ✓
NO WAY to know which outputs are “change” and which are Recipient addresses

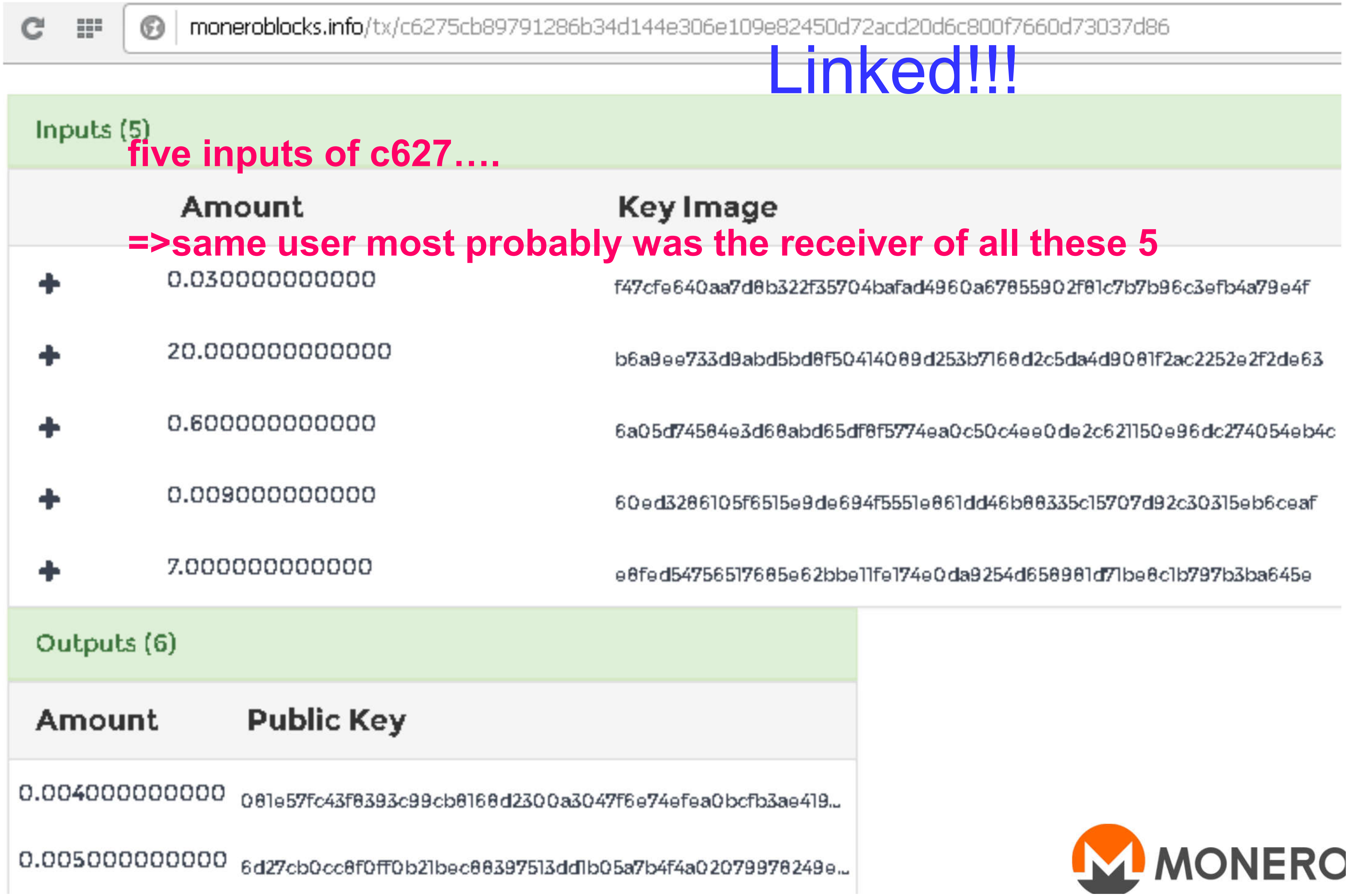


Pb3.

FRAGMENTATION=>



=>these 2 outputs ARE LINKED at this later stage!!



moneroblocks.info/tx/c6275cb89791286b34d144e306e109e82450d72acd20d6c800f7660d73037d86

Linked!!!

Inputs (5)

five inputs of c627….

=>same user most probably was the receiver of all these 5

	Amount	Key Image
✚	0.030000000000	f47cfe640aa7d8b322f35704bafad4960a67855902f81c7b7b96c3efb4a79e4f
✚	20.000000000000	b6a9ee733d9abd5bd8f50414089d253b7168d2c5da4d9081f2ac2252e2f2de63
✚	0.600000000000	6a05df74584e3d68abd65df8f5774ea0c50c4ee0de2c621150e96dc274054eb4c
✚	0.009000000000	60ed3286105f6515e9de694f5551e861dd46b88335c15707d92c30315eb6ceaf
✚	7.000000000000	e8fed54756517685e62bbe11fe174e0da9254d658981df71be8c1b797b3ba645e

Outputs (6)

Amount	Public Key
0.004000000000	081e57fc43f8393c99cb8168d2300a3047f6e74efea0bcfb3ae419...
0.005000000000	6d27cb0cc8f0ff0b21bec88397513dd1b05a7b4f4a02079978249e...

Blockchain Anonymity

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

⇒ WRONG:

- **Asymmetry of information market manipulation and big data used by dishonest competitors.**

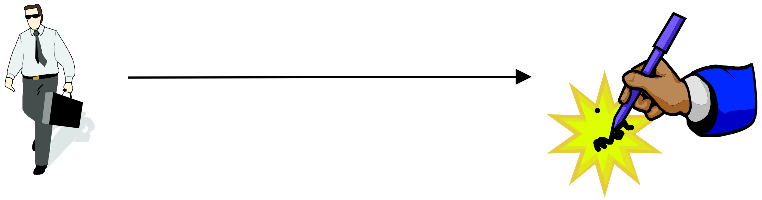
Blockchain technology WILL NEVER be adopted by banks if it INCREASES the disclosures => need for anonymity solutions.

- **Ring signatures.**
- **Zero knowledge proofs.**
- **Confidential Transactions [CT]**
- **Other advanced crypto, e.g. attribute-based encryption.**

Digital Signatures – 1 Signer

0. Completeness – **honest signer always accepted**

1. Soundness – **dishonest signer always rejected**



Group Signatures

pk_A, sk_A
pk_B, sk_B
pk_C, sk_C
pk_D, sk_D
Group 1

0. Completeness – **honest signer always accepted**

1. Soundness – **dishonest signer always rejected**

2. Anonymity – **the verifier does not know who signed!**

signer ABCD

Group Signatures-Big Brother Syndrome

⇒ **Centralized: a group leader/manager sets it up**

  ⇒ **Single Point of Failure**

⇒ **Trace-able:**
most schemes ALLOW to remove anonymity [by the manager].

⇒ **Not flexible: groups are defined beforehand**

⇒ **Not permission-free: nobody will force me to be a part of group.**

Ring Signatures – Very Different

- ⇒ De-Centralized: no group manager
  - ⇒ Next weak point: it is sufficient to “crack” one key
- ⇒ In most schemes THERE IS NO WAY to remove anonymity
- ⇒ Super flexible: ad-hic groups not defined beforehand
- ⇒ Permission-less: I can be involved in one signature without doing anything
- ⇒ Deniable: it was not me… contrary of Non-repudiation/Imputability.

-Problems: there are ways to comprise anonymity: backdoors, covert channels…

-Potentially legal problems [Satoshi Nakamoto vs UK Law]

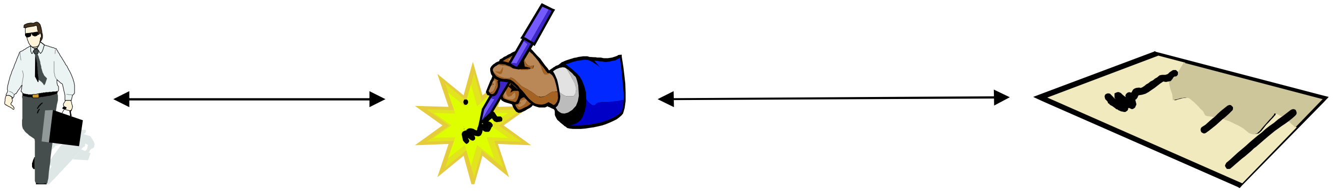
Main currency:
XMR = Monero, 20 M$ market cap@0716, 8x increase in 2 weeks.

Electronic Signatures – EU Directive 1999

1. Electronic Signature.

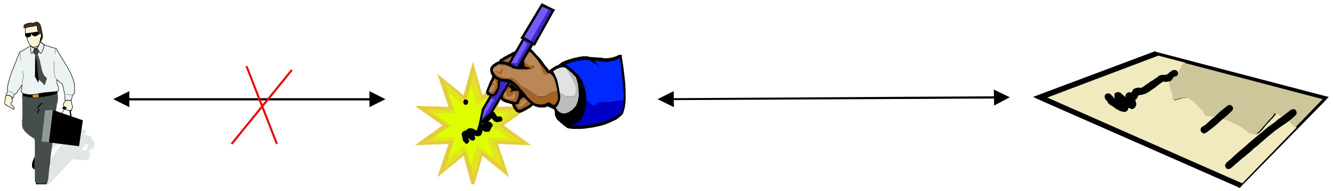
2. Advanced Electronic Signature.

2x link.



Ring Signatures - Unlinkable

1x link.

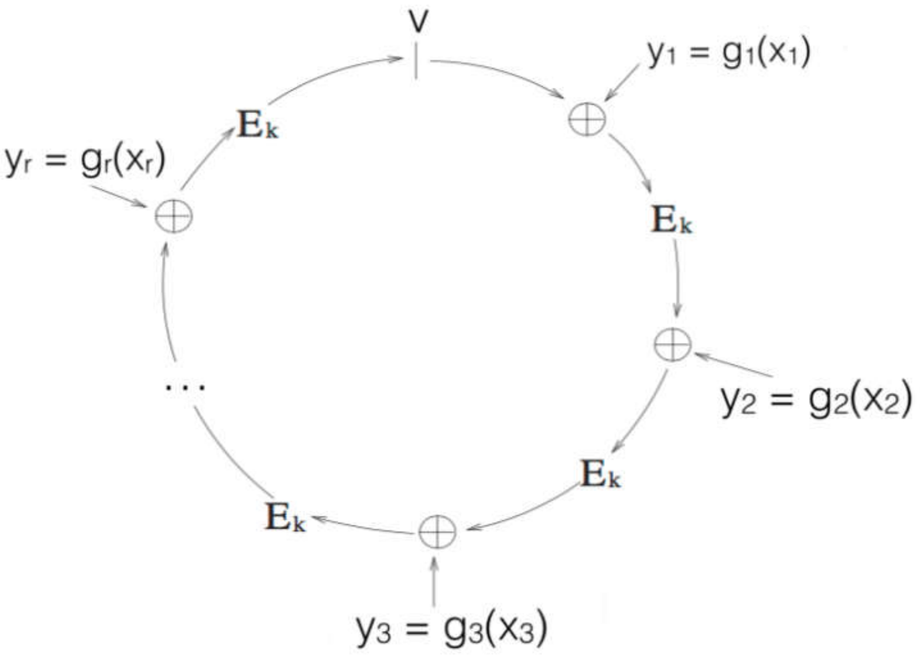


Ambiguity: several signers are “equally probable”

Unconditional Unlinkability

RST-style Ring Signatures

- Based on RSA/Rabin/other Trapdoor OWF



Cryptonote Ring Signature Method

sign gen:

$$L_i = \begin{cases} q_i G, & \text{if } i = s \\ q_i G + w_i P_i, & \text{if } i \neq s \end{cases}$$

$$R_i = \begin{cases} q_i \mathcal{H}_p(P_i), & \text{if } i = s \\ q_i \mathcal{H}_p(P_i) + w_i I, & \text{if } i \neq s \end{cases}$$

non-interactive *challenge*:

$$c = \mathcal{H}_s(m, L_1, \ldots, L_n, R_1, \ldots, R_n)$$

the *response*:

$$c_i = \begin{cases} w_i, \ \text{random} & \text{if } i \neq s \\ c - \sum_{i=0}^{n} c_i \mod l, & \text{if } i = s \end{cases}$$

$$r_i = \begin{cases} q_i, \ \text{random} & \text{if } i \neq s \\ q_s - c_s x \mod l, & \text{if } i = s \end{cases}$$

$$\sigma = (I, c_1, \ldots, c_n, r_1, \ldots, r_n).$$

a One-Time/Linkable Ring Signature

based on ECDL, a form of NIZK

with n challenges c_i and n responses r_i

verif:

$$\begin{cases} L_i' = r_i G + c_i P_i \\ R_i' = r_i \mathcal{H}_p(P_i) + c_i I \end{cases}$$

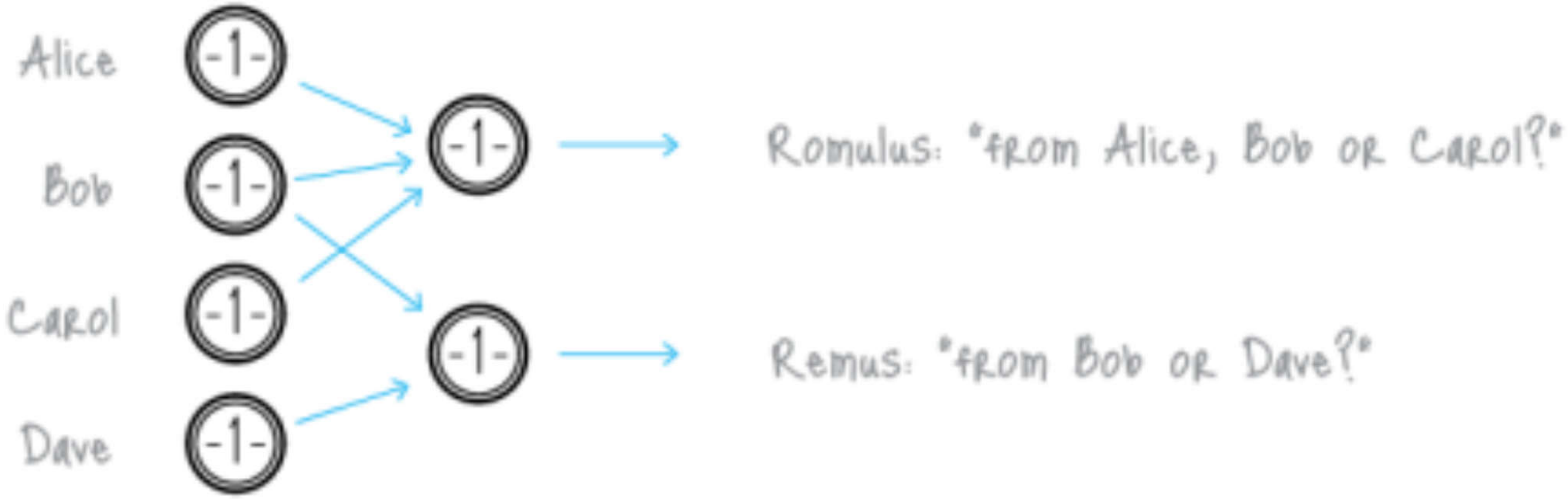
check

$$\text{if } \sum_{i=0}^{n} c_i \stackrel{?}{=} \mathcal{H}_s(m, L_0', \ldots, L_n', R_0', \ldots, R_n') \mod l$$

(each user has a different way to satisfy this condition)

Linkable Ring Signatures

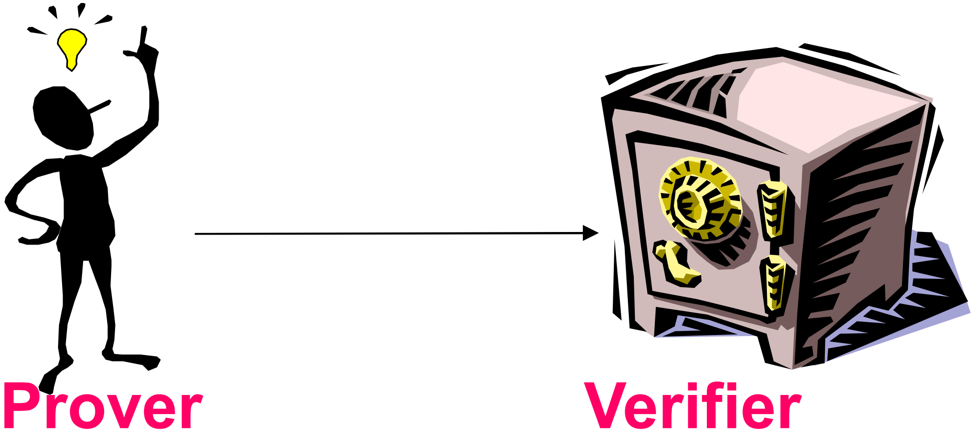
- Linking signatures by the same signer, with no revocation of anonymity!
- Needed to prevent double-spending.



Alice
Bob
Carol
Dave
-1-
-1-
-1-
-1-
-1-
-1-
Romulus: "from Alice, Bob or Carol?"
Remus: "from Bob or Dave?"

Zero Knowledge

Zero-Knowledge



0. Completeness –
honest signer always accepted

1. Soundness –
dishonest signer always rejected

2. Zero-Knowledge –
the verifier does not learn ANYTHING

Zerocoin/Zerocash

ZeroCoin [Green et al. 2013]

Anonymity by destruction / creation of basecoins:

- Destroy 1 basecoin unit.
- ZK prove that you had it.
- The system agrees to re-create one basecoin.

money remains visible…

ZeroCash [Green et al. 2014]

- amounts and mixing also invisible!

=>claimed 1st to achieve real untrace-ability

=>ZEC went live 28 Oct 2016!

Zerocoin Basic Principles

S secret serial number,

r secret random “one-time private key” needed to spend S later on

$H=g^S h^r$ = the commitment published on the blockchain (≈creation of 1 ZC)

This serial number S is for accounting [avoid double spending],

Now revealing this serial number S will be worth 1 BTC,

IF we can prove we know r which remains secret at all times.

like one-time signature mechanism.

PROBLEM: Breaks bitcoin, requires permission of devs+miners for creation of bitcoins out of thin air

ZK Proof

A ZK proof that you have 1 valid coin:

to spend S we produce a short ZK proof of:

Not totally different than a ring signature:

No message to sign, but
ANY out of many owners of some coin
can produce it.

Size(proof)=log(#users).

I know r such that

$H_1=g^S h^r$

or

$H_2=g^S h^r$

or

$H_3=g^S h^r$

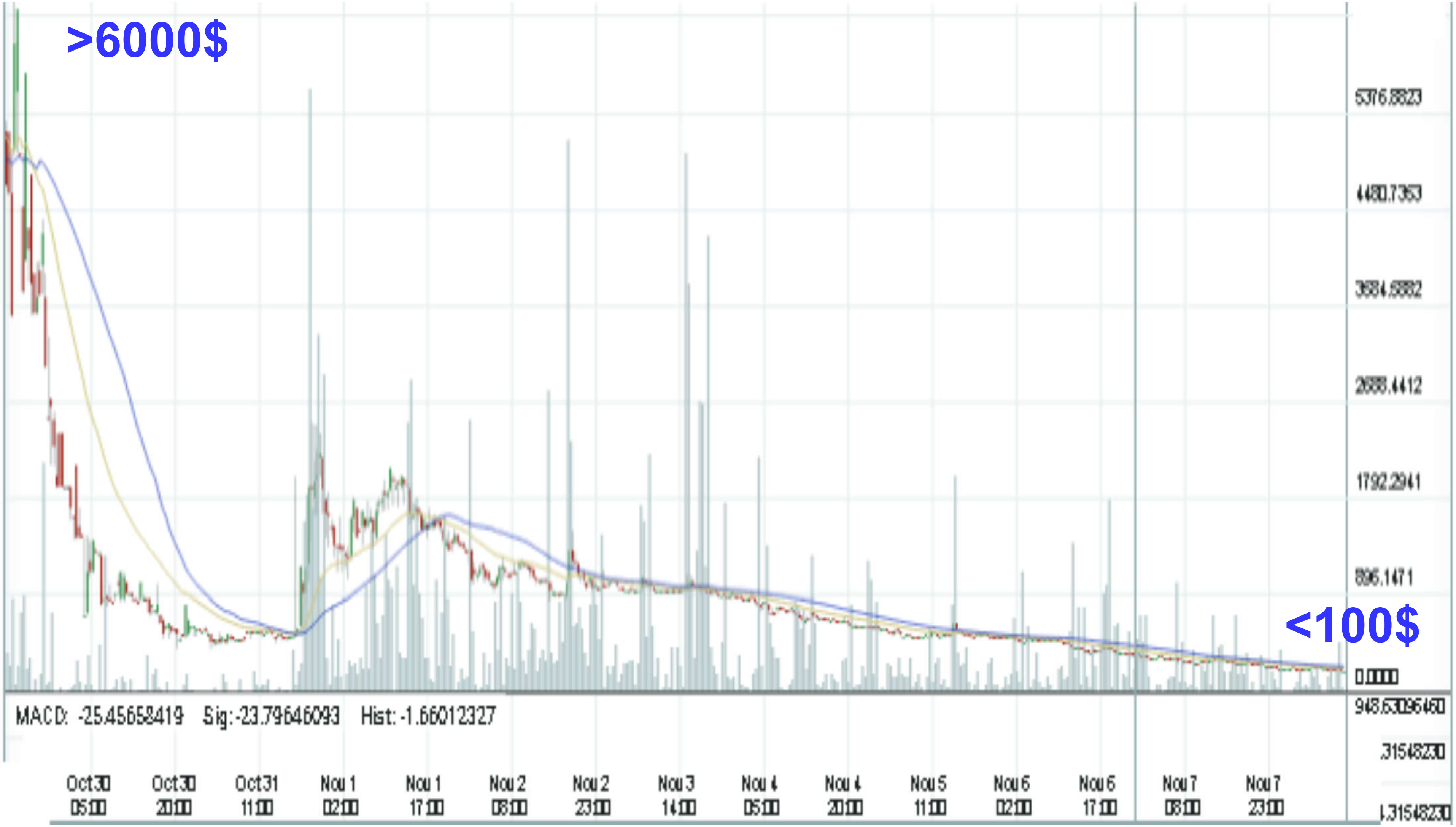
or

…

huge disjunction,
up to for ALL existing coins

Delusion ≠ Greatness

- ZeroCash has already attracted a lot of criticism.



>6000$

<100$

"Cryptographer's Job"

- Claim:
  - Blockchains do need A LOT MORE of "good" cryptography to be widely adopted.
  - We need more
    - security
    - privacy
    - speed
  - Most current blockchains have serious problems.