The Blockchain Revolution

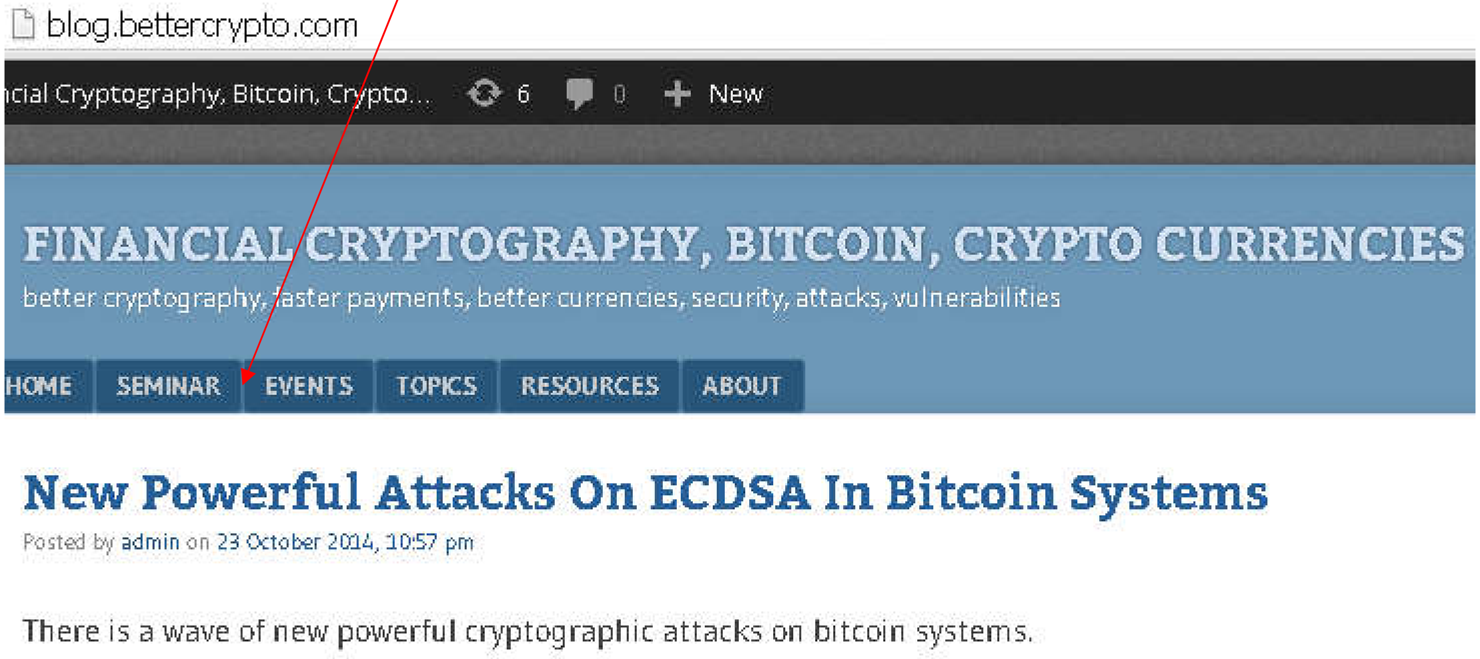
Nicolas T. Courtois

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

UCL RESEARCH CENTRE FOR BLOCKCHAIN TECHNOLOGIES

Blockchain Events@UCL

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.

Our Work

-see 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

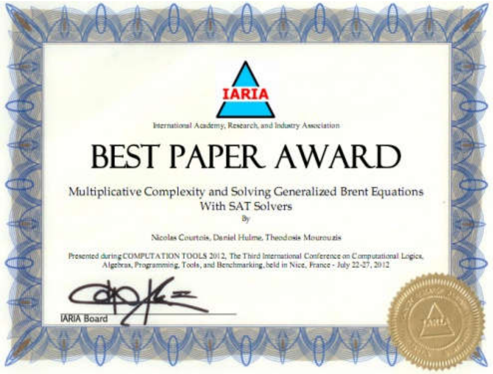
-Nicolas T. Courtois, Pinar Emirdag and Daniel A. Nagy: Could Bitcoin Transactions Be 100x Faster? In proceedings of SECRYPT 2014, 28-30 August 2014, Vienna, Austria.

-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

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

“Cryptographer’s Dream”

- Building “trust-less” systems.

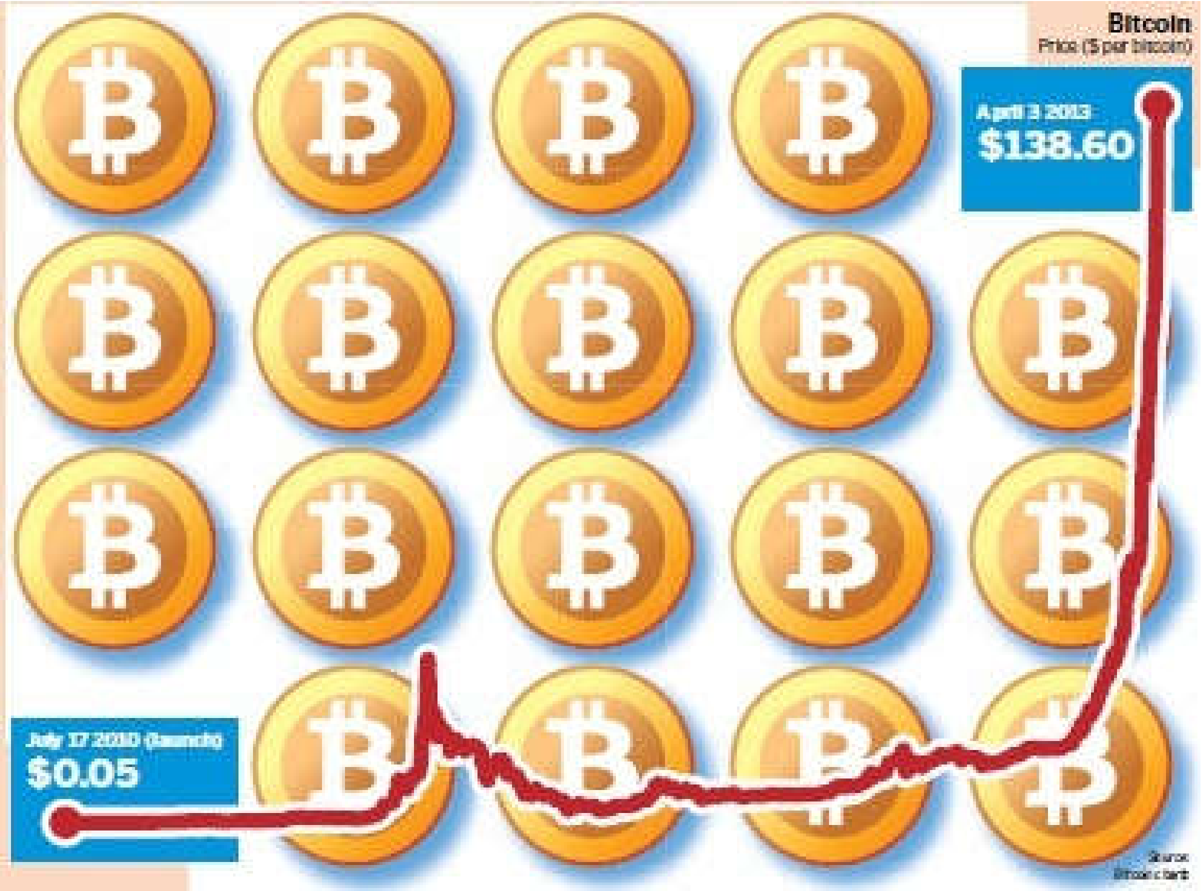
no need for lawyers, notaries, policemen, etc…

crypto “magic”

FINANCIAL TIMES

USA Thursday April 4 2013

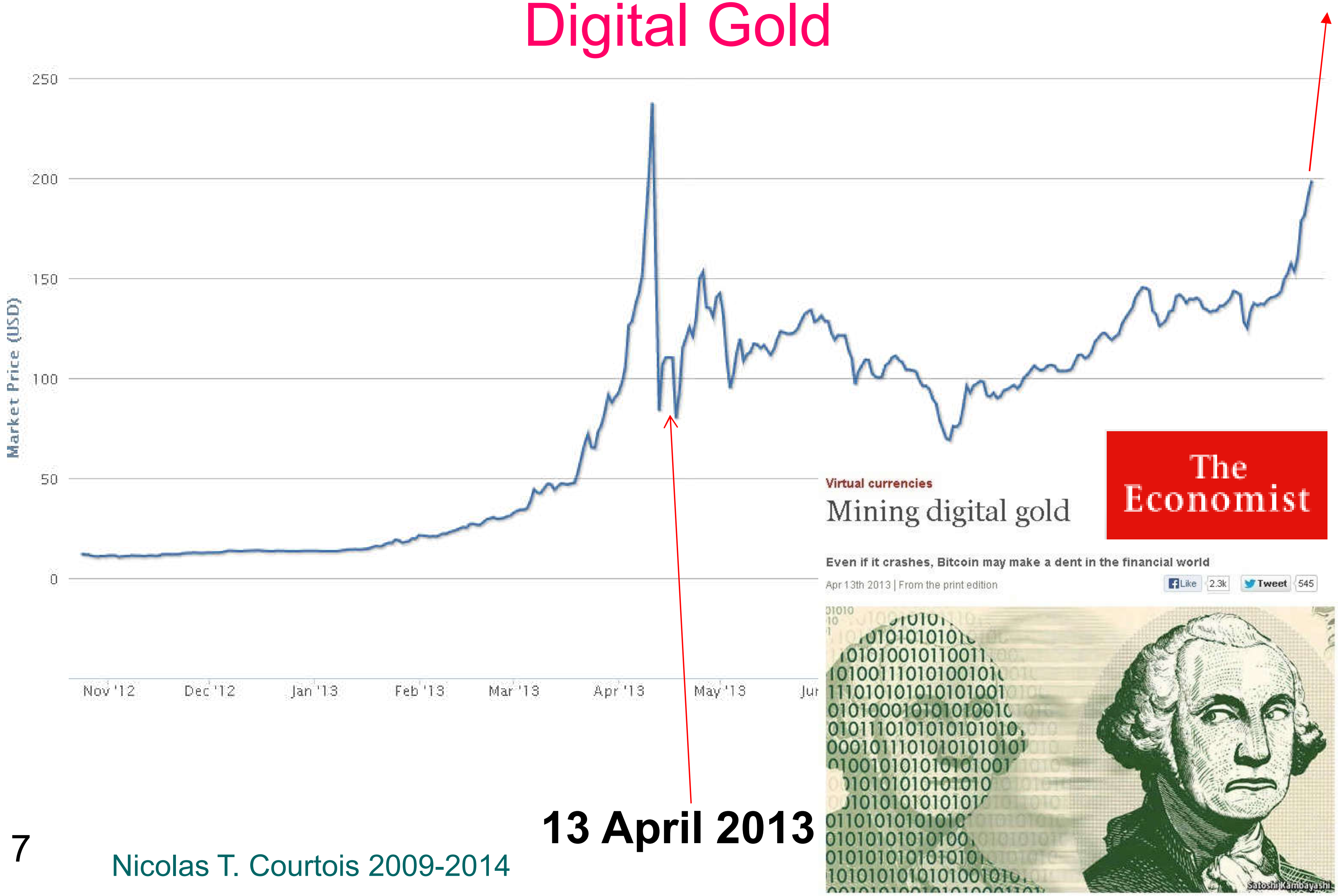
Buying frenzy sends virtual currency on way to becoming next bubble



bubble?

it was just the beginning…

Digital Gold



Virtual currencies

Mining digital gold

The Economist

Even if it crashes, Bitcoin may make a dent in the financial world

Apr 13th 2013 | From the print edition

Like 2.3k Tweet 545

13 April 2013

Digital Anarchy

- 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

**Citations

Bitcoin is:

- Wild West of our time [Anderson-Rosenberg]
- There is no “undo” button for sth. like bitcoin [Mike Gogulski]

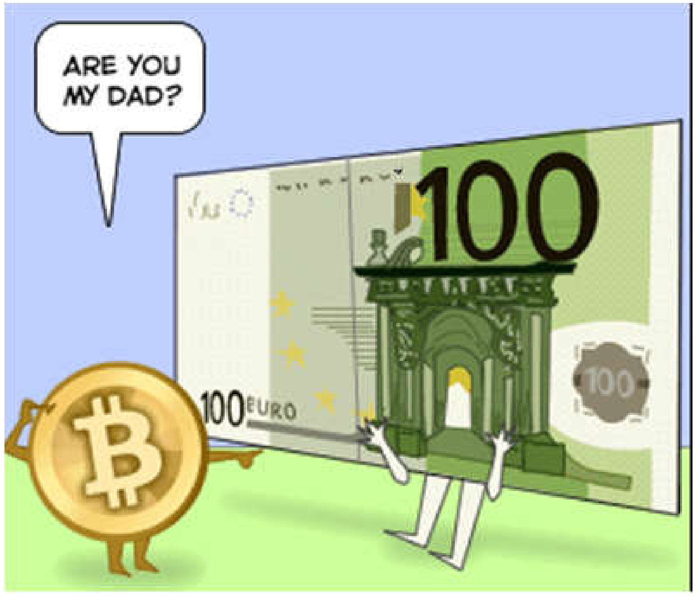
Bitcoin vs. Stock Markets

Wall Street lawyer citations:

- “bitcoin technology is brilliant“ and maybe
- a “kind of value transfer network that you could dream about creating” for the stock markets
  - “if existing businesses had the luxury of a fresh start”

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

Bitcoin



Bitcoin

Based on cryptography and network effects.

Private money.

Bitcoin

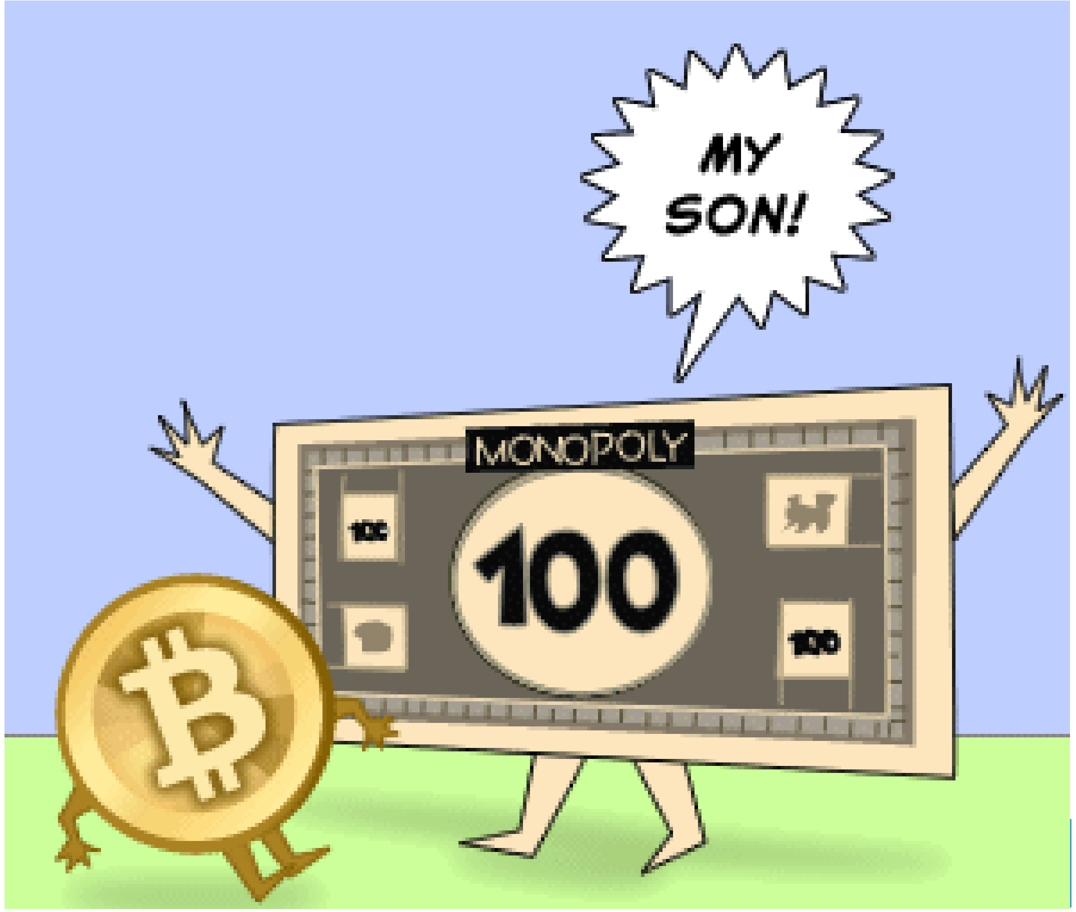
Bitcoins are cryptographic money

- 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)

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)

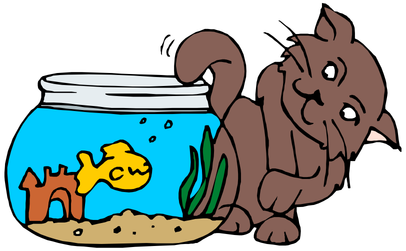
PK A

public ledger says H(PK A) has 1 BTC

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

Authorizing Transfer of Coins

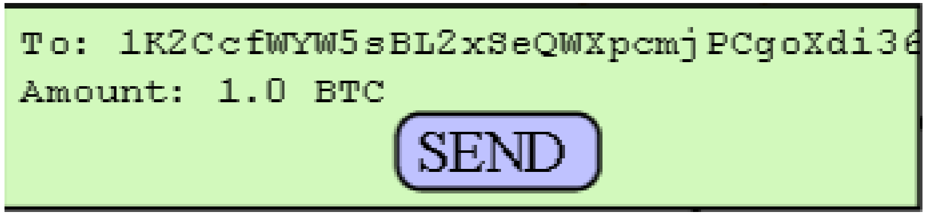
- you have a private key => you have the money (right to transfer)
  - money stored on PCs or mobile phones?



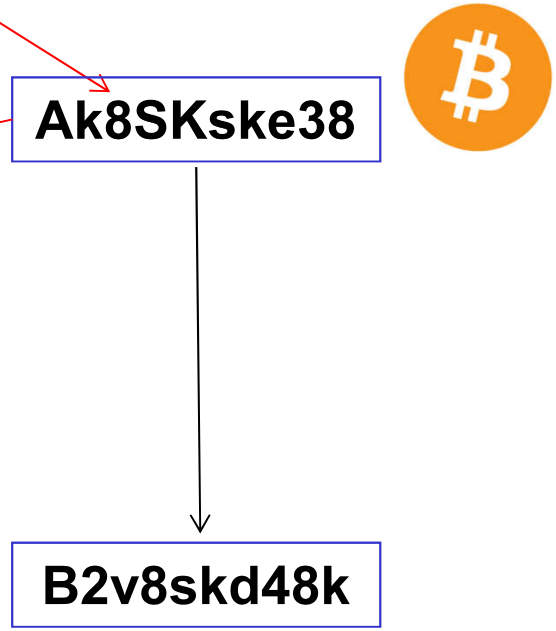
  - better solution: smart card

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

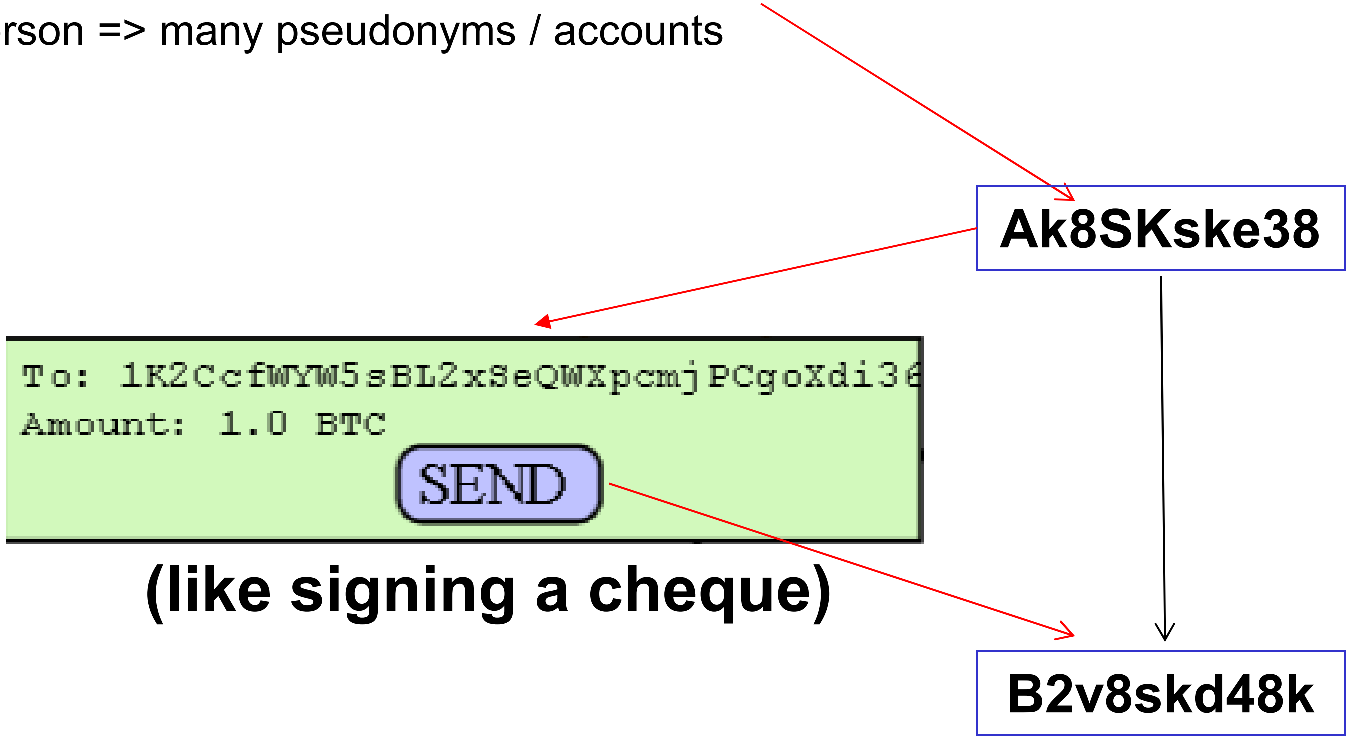


```
To: 1K2CcfWYW5sBL2xSeQWXpcmjPCgoXdi36
Amount: 1.0 BTC
```



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)

Trust Less!

Digital Signatures ENABLE
these TRUSTLESS systems!

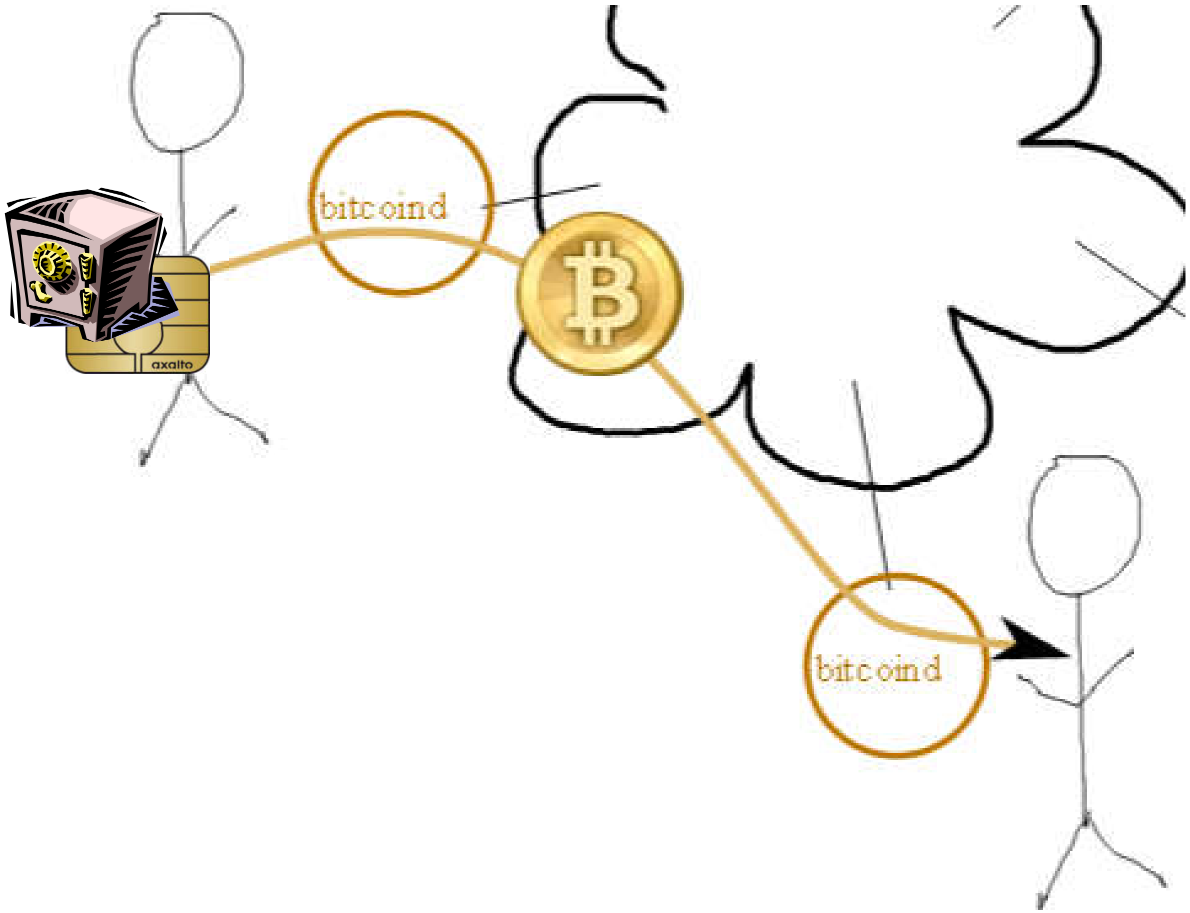
Example: My bank card signs a transaction with RSA, the bank does NOT know the private key,
ONLY the public key.

⇒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 chip and PIN bank card



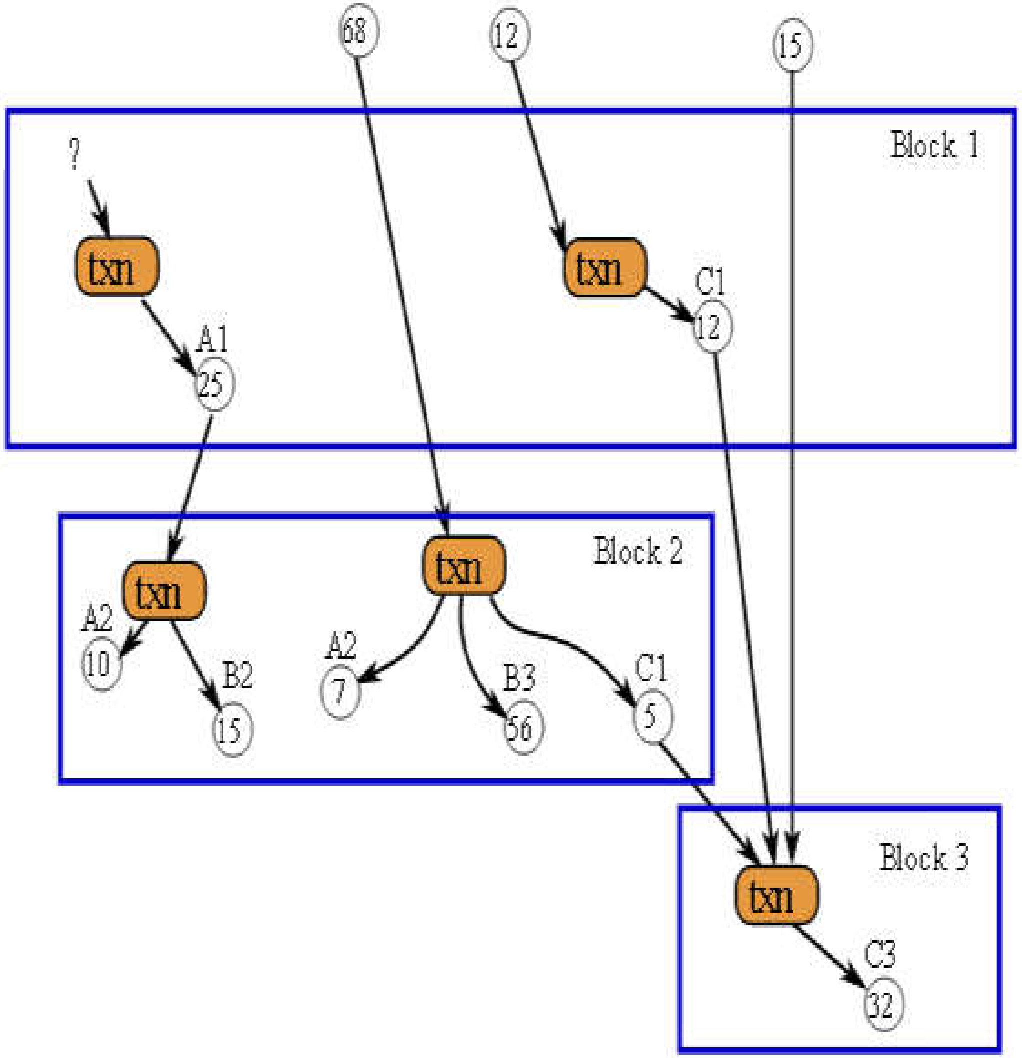
Block Chain

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)



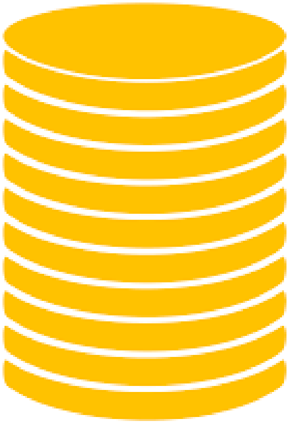
Multiple Confirmations

=>each new block confirms
ALL previous events

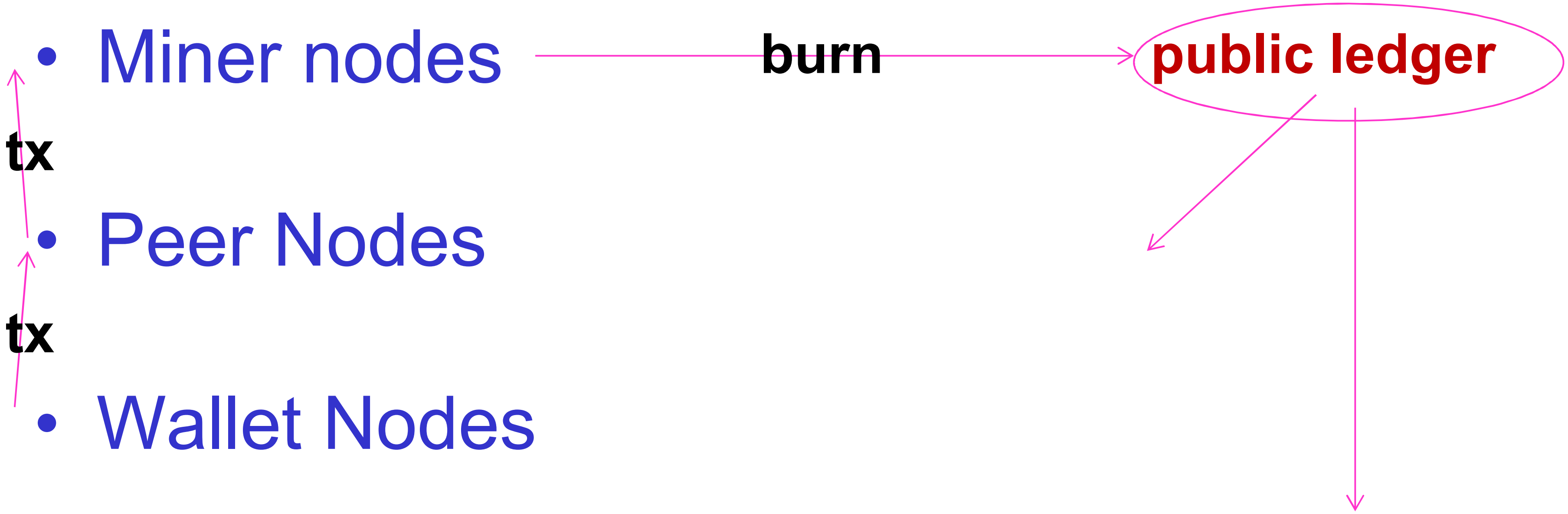
Security:

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

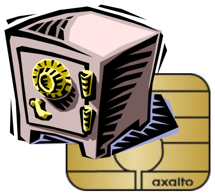
- evidence piles up
- with time it becomes too costly to cheat



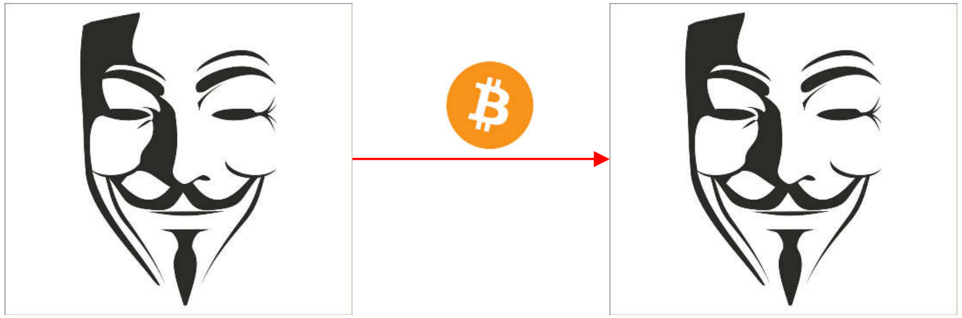
Tx LifeCycle



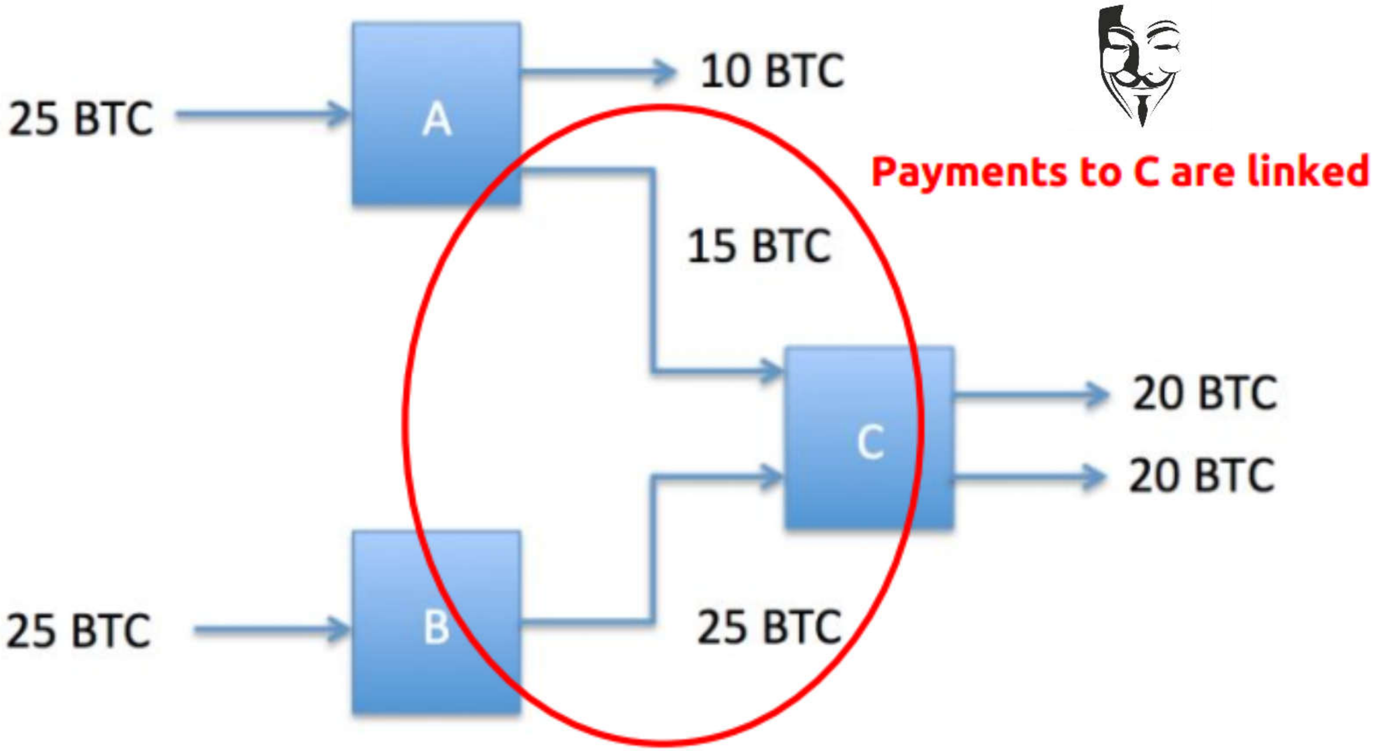
- Miner nodes
- Peer Nodes
- Wallet Nodes



anonymous payments

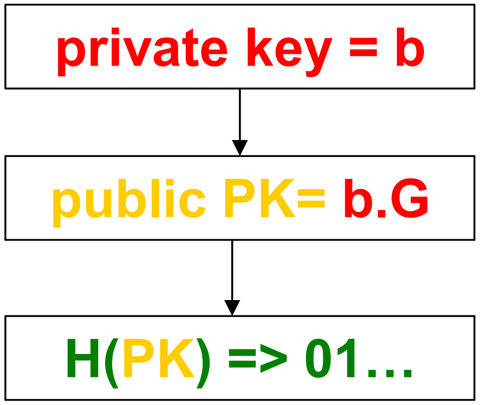


Bitcoin and Linakability



Q: Does Monero/ZeroCash remove this????

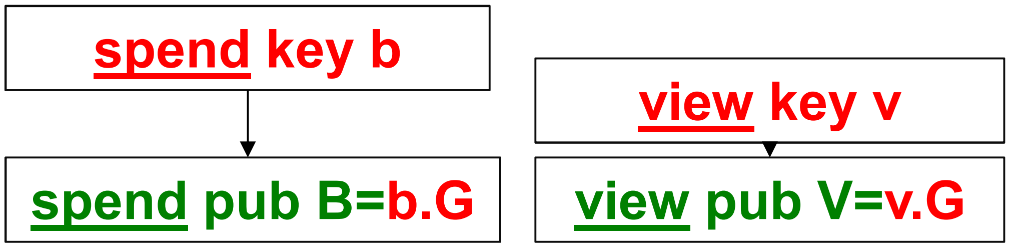
Bitcoin vs. Monero



private key = b

public PK= b.G

H(PK) => 01…

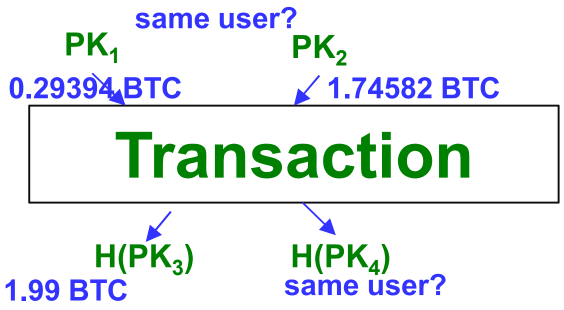


spend key b

spend pub B=b.G

view key v

view pub V=v.G



same user?

PK_1

PK_2

0.29394 BTC

1.74582 BTC

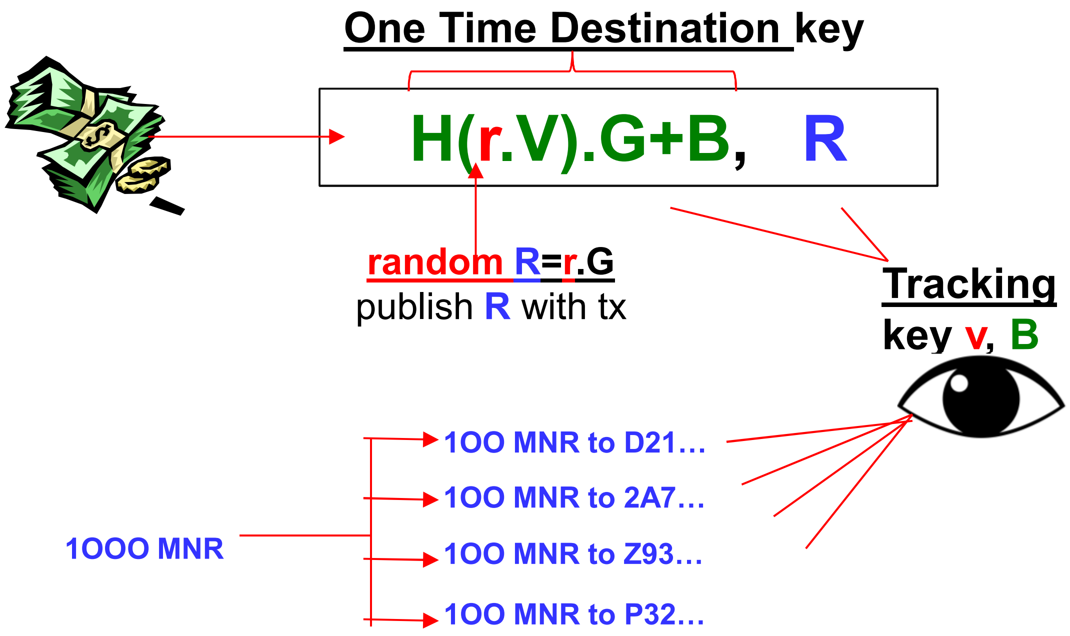
Transaction

$H(PK_3)$

1.99 BTC

$H(PK_4)$

same user?



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…

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:

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

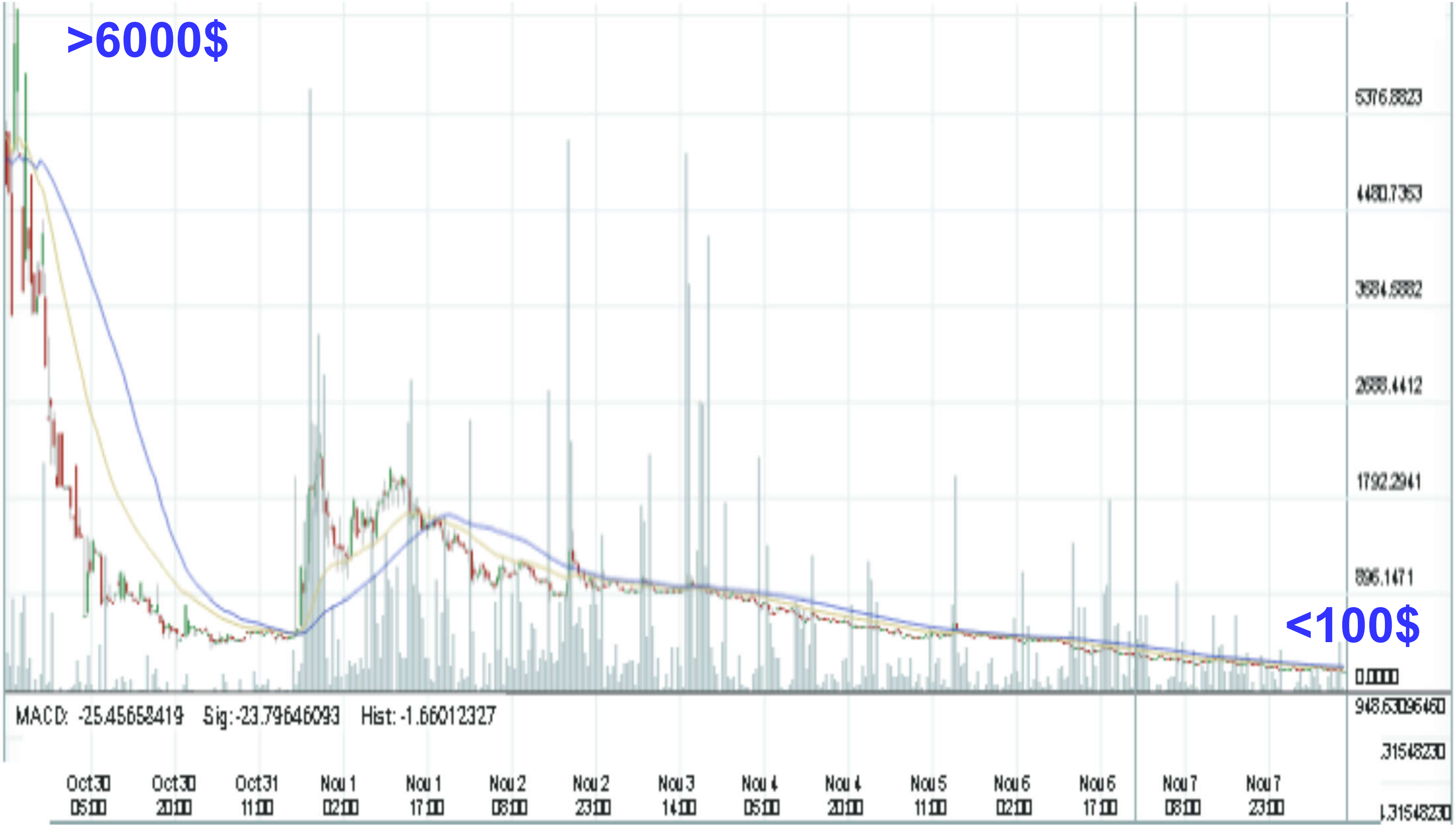
…

Hides the origin of moneys,

1 out of 1 Million!!

Delusion ≠ Greatness

- ZeroCash has already attracted a lot of criticism.



>6000$

<100$