Overview of Blockchain Security

- speed=>security -

Nicolas T. Courtois

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

UCL RESEARCH CENTRE FOR BLOCKCHAIN TECHNOLOGIES

Hegel [1770-1831], German philosophy

The history
is the process
of broadening
freedom.

For Years I Thought That..

$$\text{Freedom} \rightarrow \infty$$

$$\Rightarrow$$

$$\text{Security} \rightarrow 0$$

Freedom ⇒ Security issues…

Examples:

- invention of train
  ⇒ pickpockets
- car traffic:
  ⇒ major cause of death (2M/year)
- invention of the internet
  ⇒ pirates and hackers

Need For Speed

http://video.ft.com/3667480923001/Camp-Alphaville-on-cashless-society/Editors-Choice,
2 July 2014.

At minute 02.48: Dr. Nicolas Courtois of UCL:

"[...]It's not true that bitcoin is 'the Internet of Money'.
Bitcoin is 'The Horse Carriage of Money'[...] “

Need For Speed – Open Problems

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 SECRYPT 2014, 28-30 August 2014, Vienna, Austria.

Poster: http://www.nicolascourtois.com/bitcoin/POSTER_100x_Secrypt2014_v1.0.pdf

Expect bitcoin scaling shake-up soon, e.g. Lighting network== Hashed TimeLock Contracts (HTLC)

Ambitious Agenda:

Freedom $\rightarrow \infty$

Speed $\rightarrow \infty$

Security $\rightarrow$ OK

Privacy $\rightarrow$ OK

2.0

Enhancements to Bitcoin:

MultiSig, SideChains, Stealth A., RingSignatures, ZK proofs, CT

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

Courtois “Theorem”

Security $\Rightarrow$ Speed

Security => Speed?

Amazing, normally security and speed are opposites.

In financial markets one can execute trades is μs.

In bitcoin we need to wait for 10 minutes and a large multiple of it for larger transactions.

Speed is slow mostly out fear of possible double spending attacks, which imposes certain precautions.

Fixing these security problems

simply allows to make bitcoin transactions much faster, or rather to accept them much earlier.

So Fix the Security Problems!

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%

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

My Blog and Bitcoin Events@UCL

blog.bettercrypto.com

“Cryptographer’s Dream”

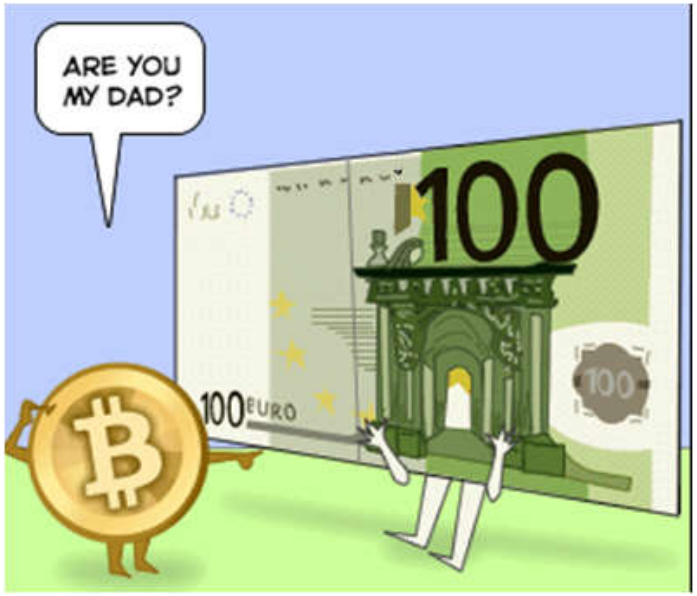
- Building “trust-less” systems and a “trust-less” society.

"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

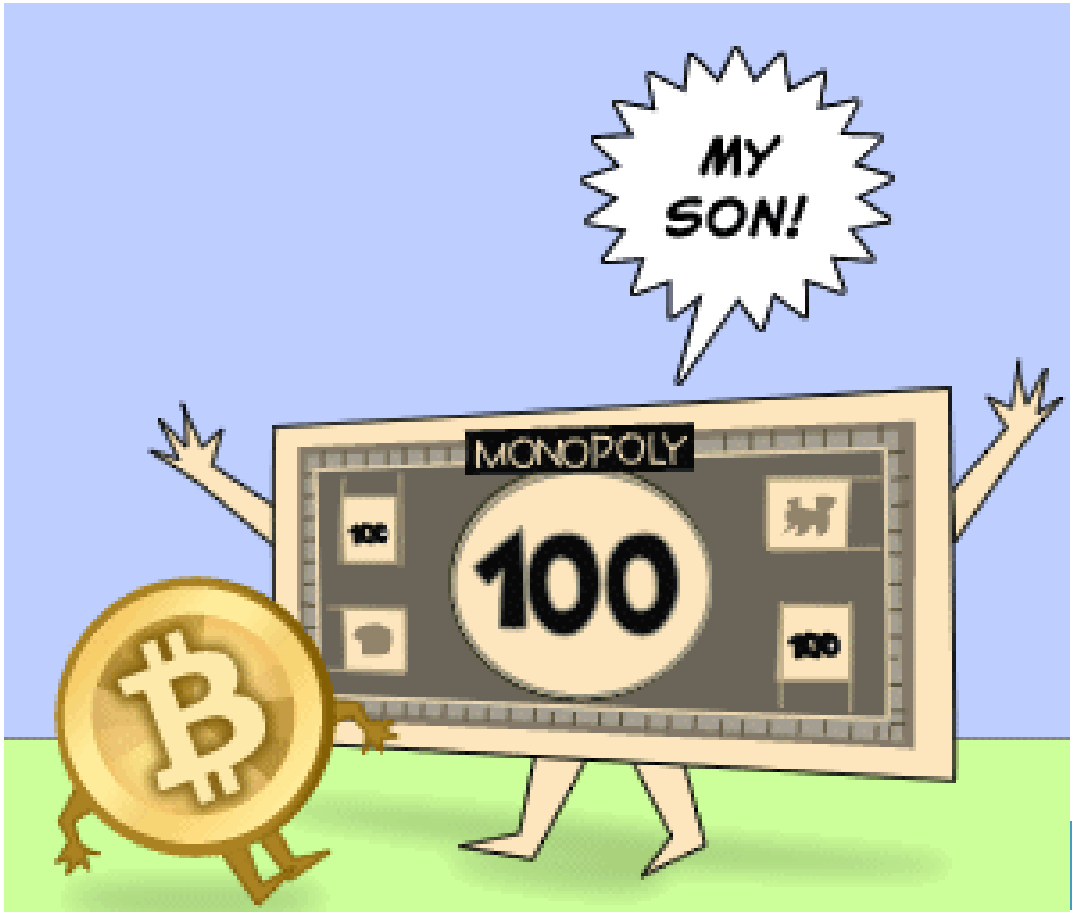
Bitcoins are cryptographic money

- 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] and Bitcoin[Nakamoto 2009]

New Coins

initially X coins are attributed through **Proof Of Work (POW)** to one public key A

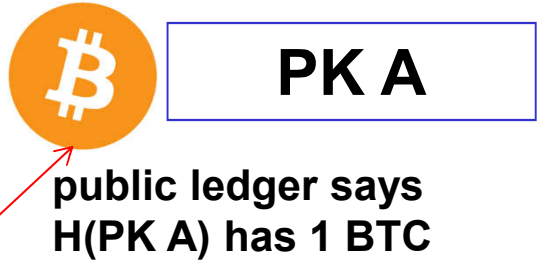
- to earn bitcoins one has to “work” (hashing) and consume energy (pay for electricity)
- do a difficult computation => you have earned 25 bitcoins
- works like a lottery (1 winner/10 minutes)

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

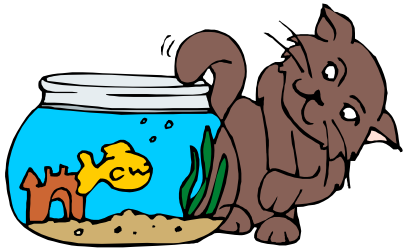
- to earn bitcoins one has to “work” (hashing) and consume energy (pay for electricity)
- do a difficult computation => you have earned 25 bitcoins
- works like a lottery (1 winner/10 minutes)



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

Authorizing Transfer of Coins

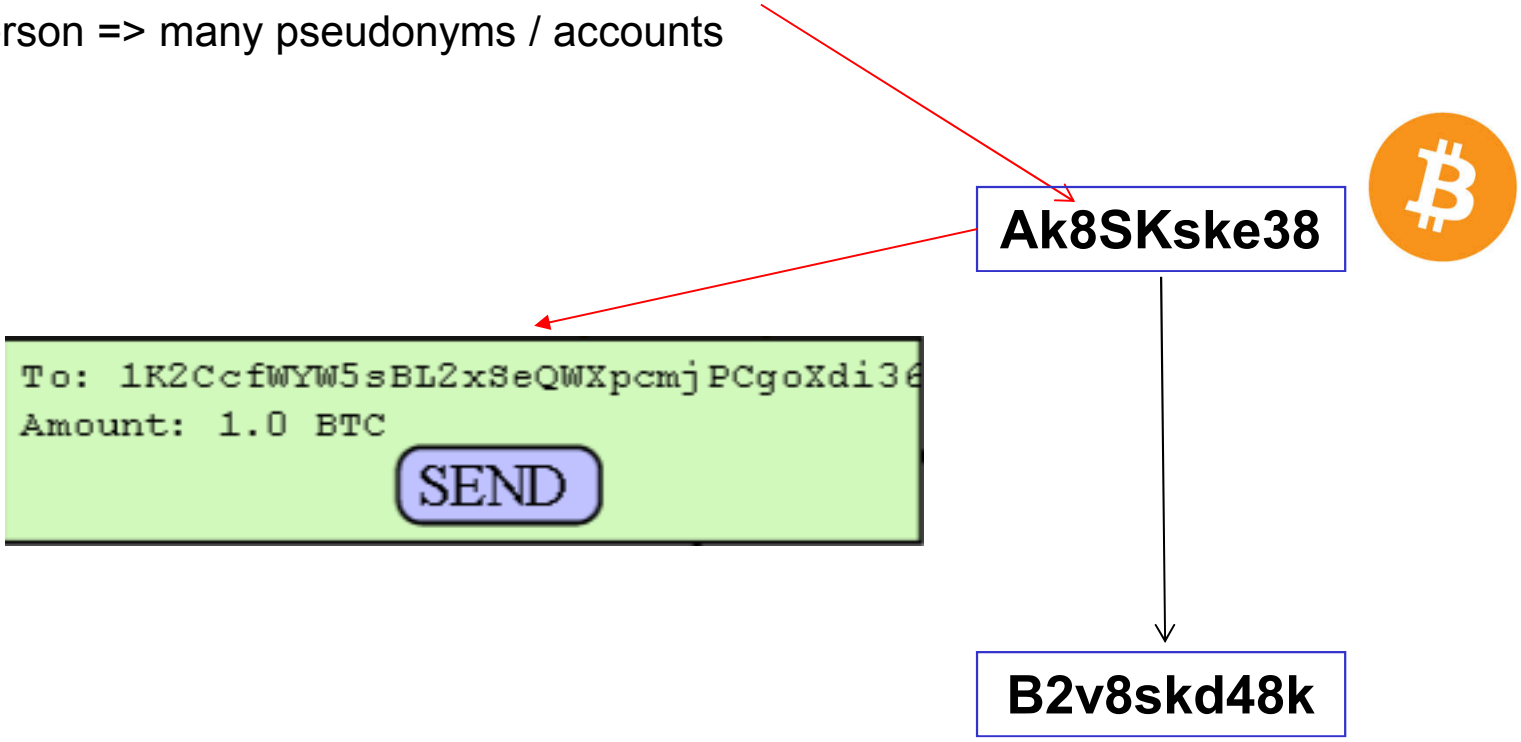
- you have a private key => you have the money (right to transfer)
  - money stored on PCs or mobile phones?



  - better solution: smart card

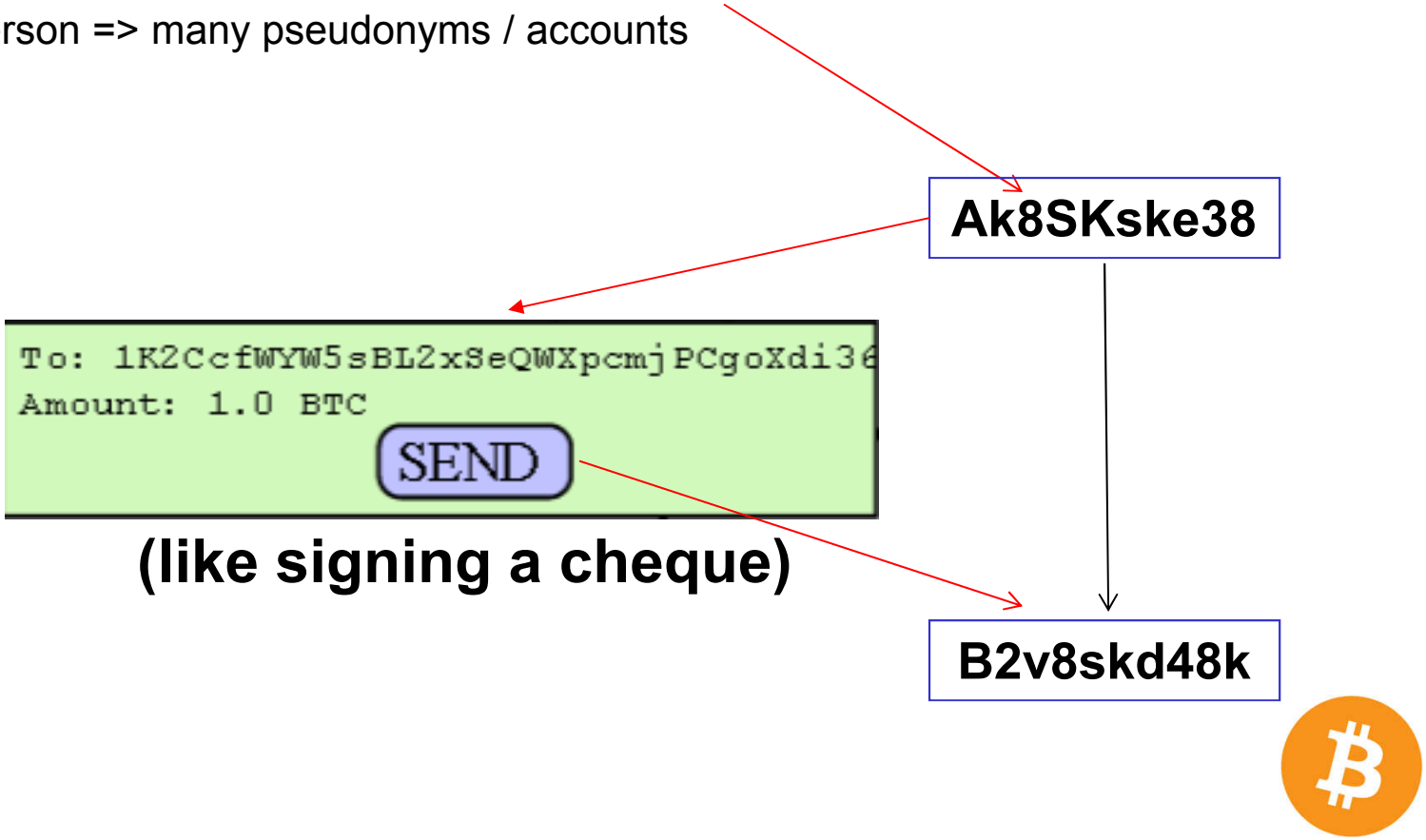
Bitcoins

- 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



Bitcoins

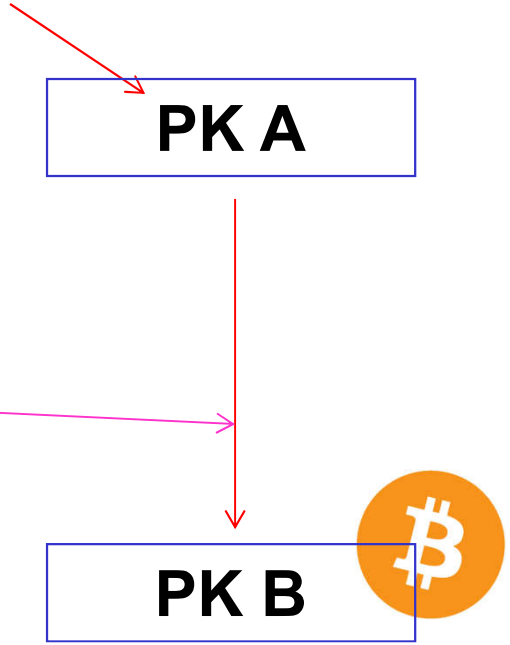
- user has the right to transfer his bitcoins to any other user
  - user are known by their pseudonyms, H(PKeys)
  - one person => many pseudonyms / accounts



Transfer of Coins

- hard work => public key A
- money transfer PK A => PK B

digital signature authorizes the transfer



Digital Signatures

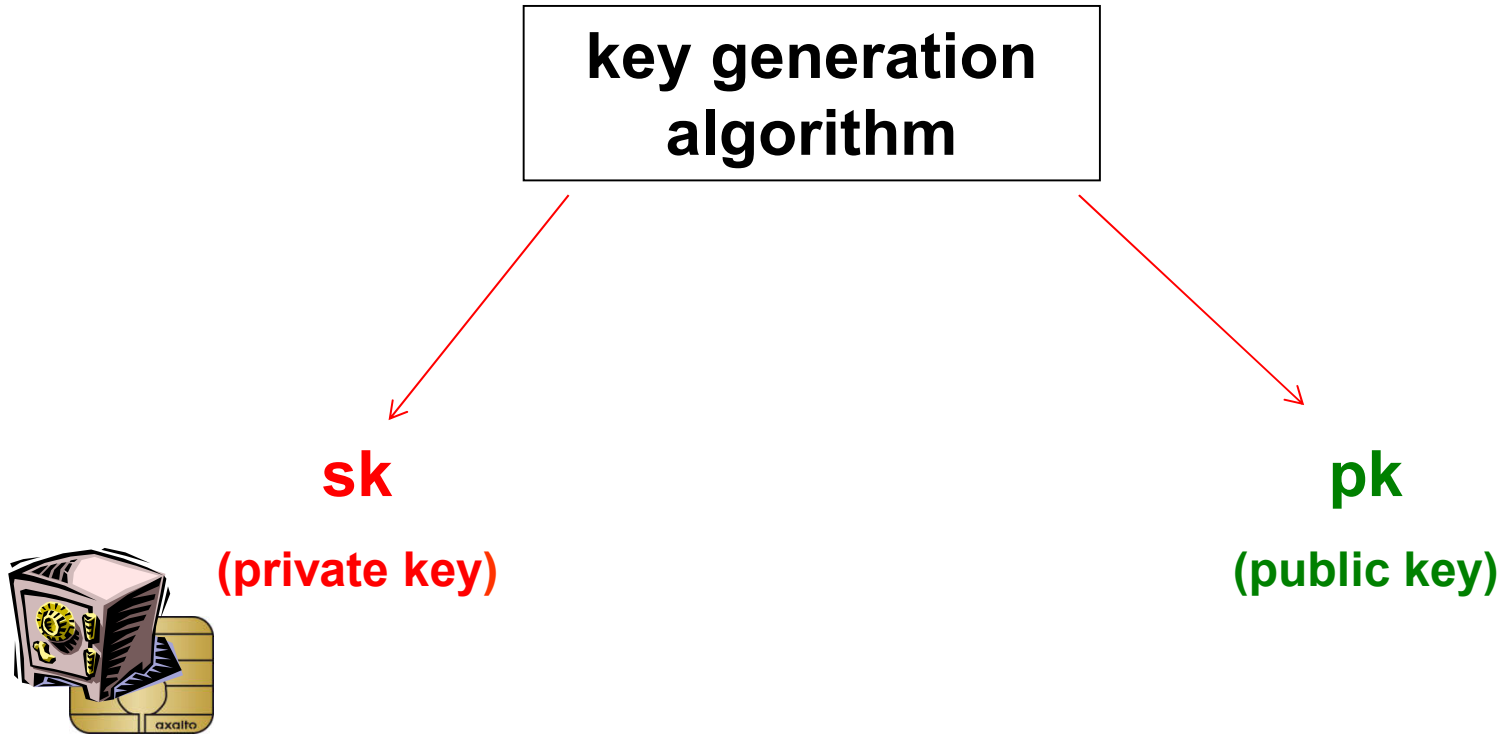
Digital Signatures

•Origin Tx(s) •Amount(s) •New Owner(s)
Signature

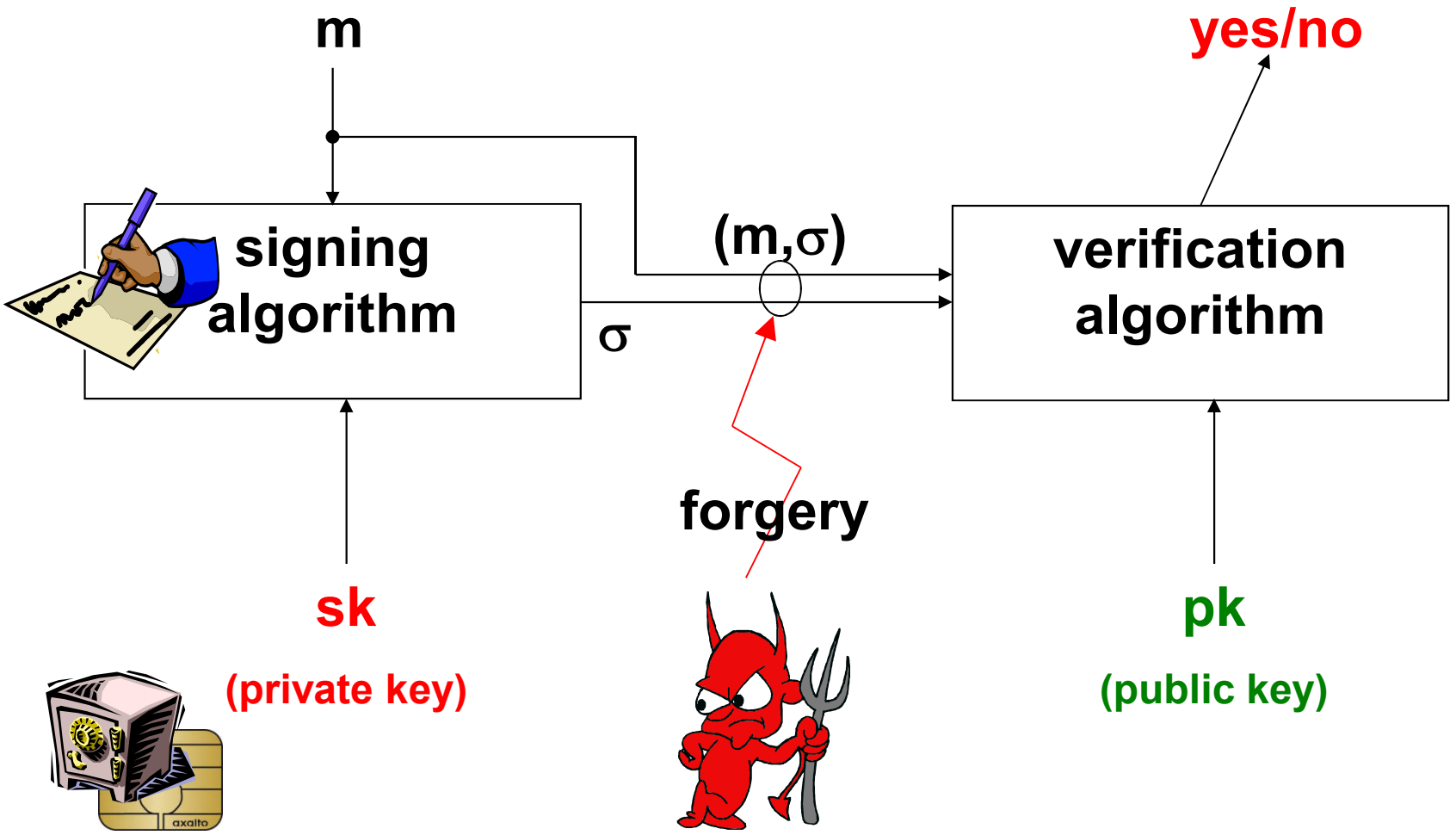
Digital Signatures

Idea: cryptographic solution

3 algorithms…



Digital Signature

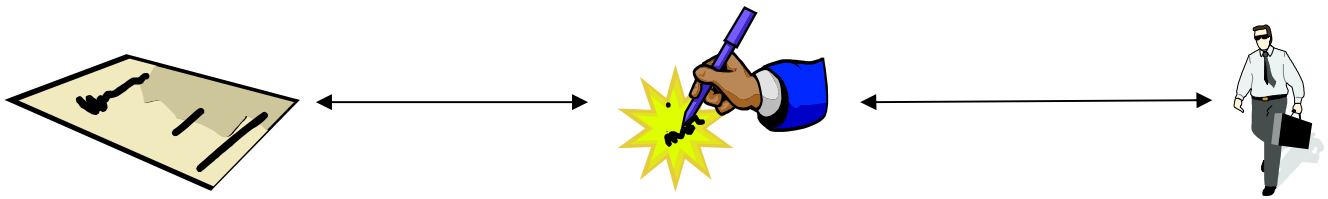


2x Link

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!

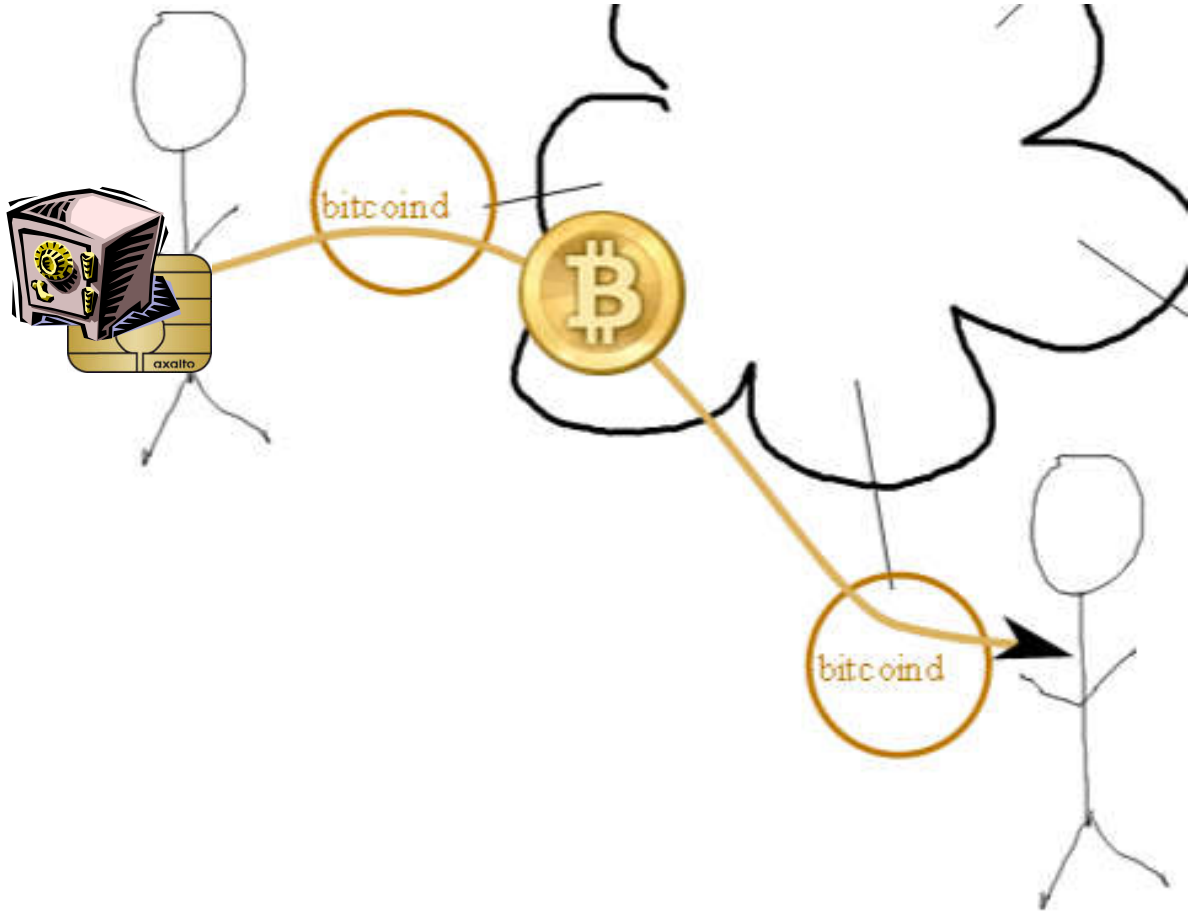
Example: My bank card signs a transaction with RSA, the bank does NOT know the private key,
ONLY the public key.

⇒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

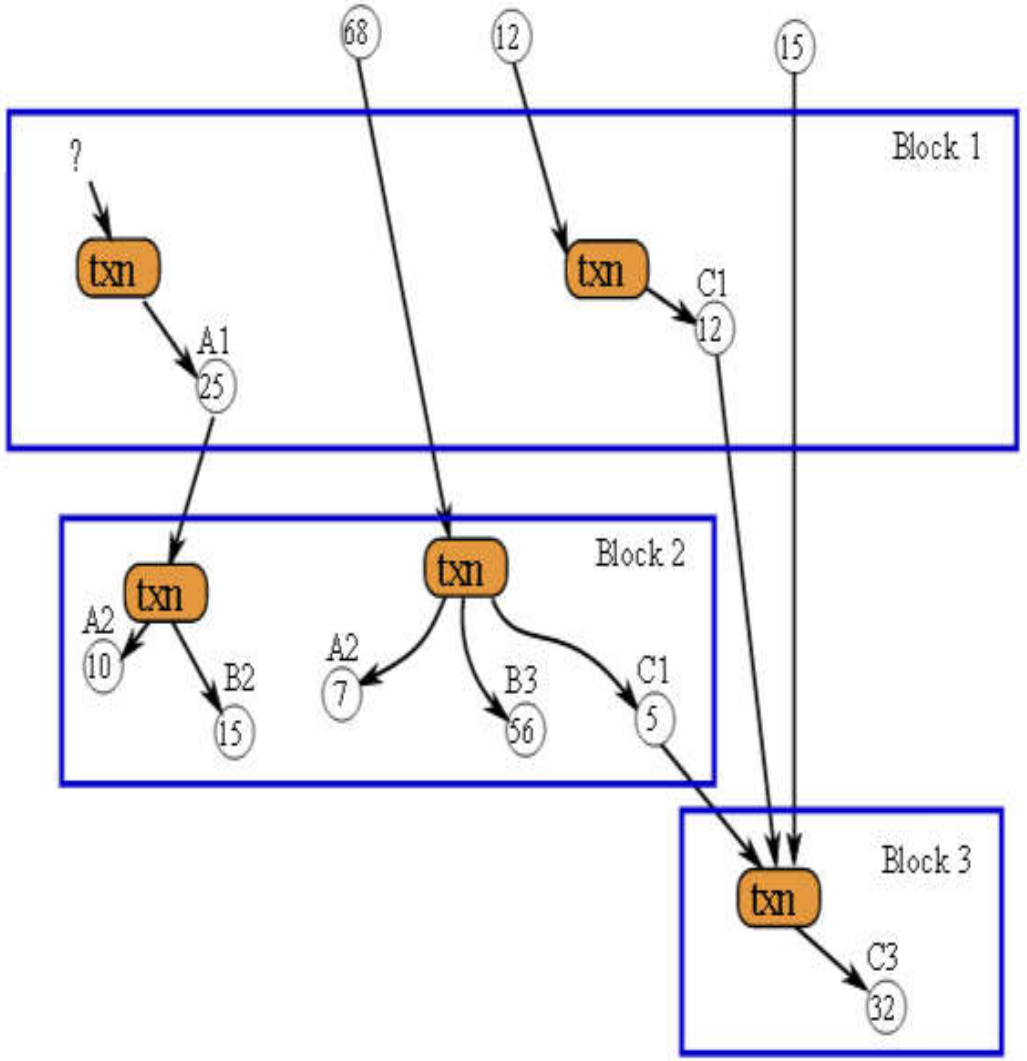
Def:

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)



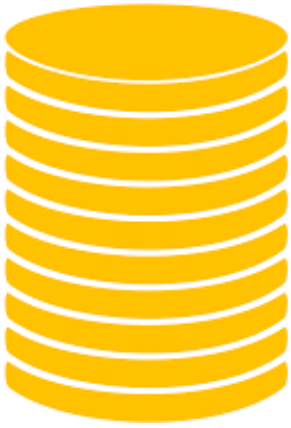
Multiple Confirmations

=>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

tx

- Peer Nodes

tx

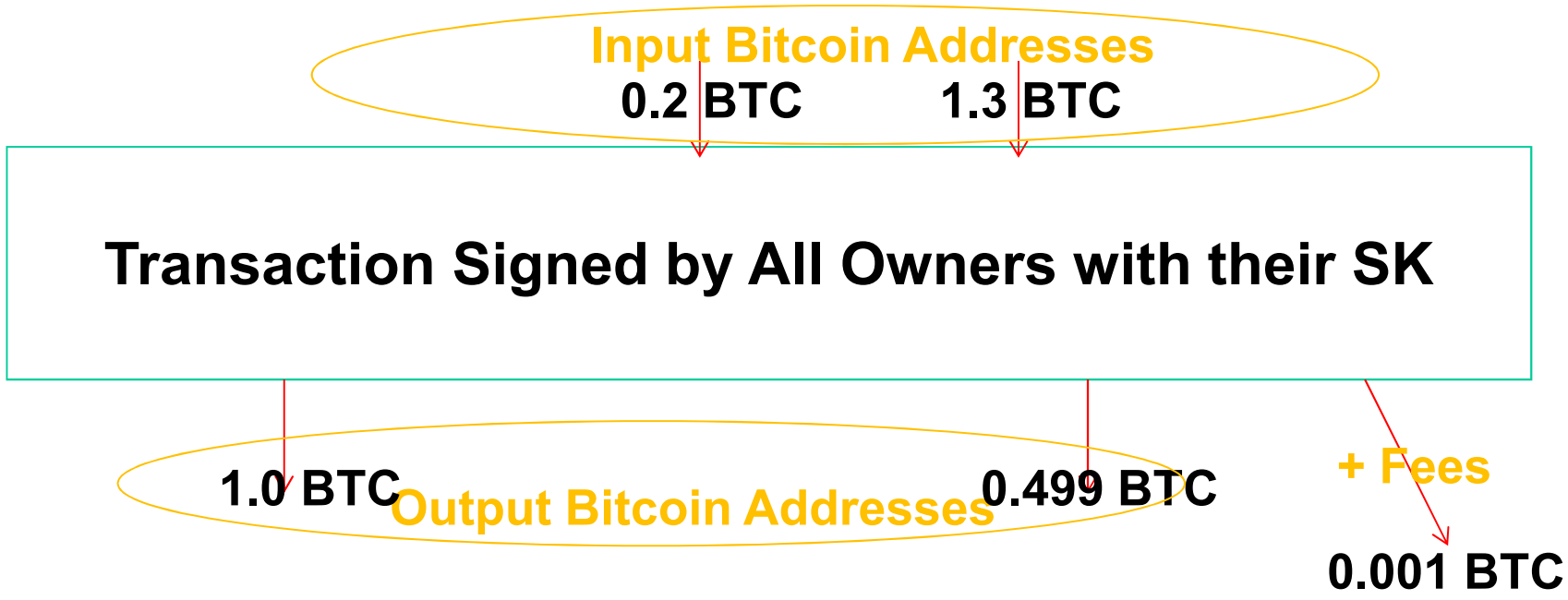
- Wallet Nodes

burn

public ledger

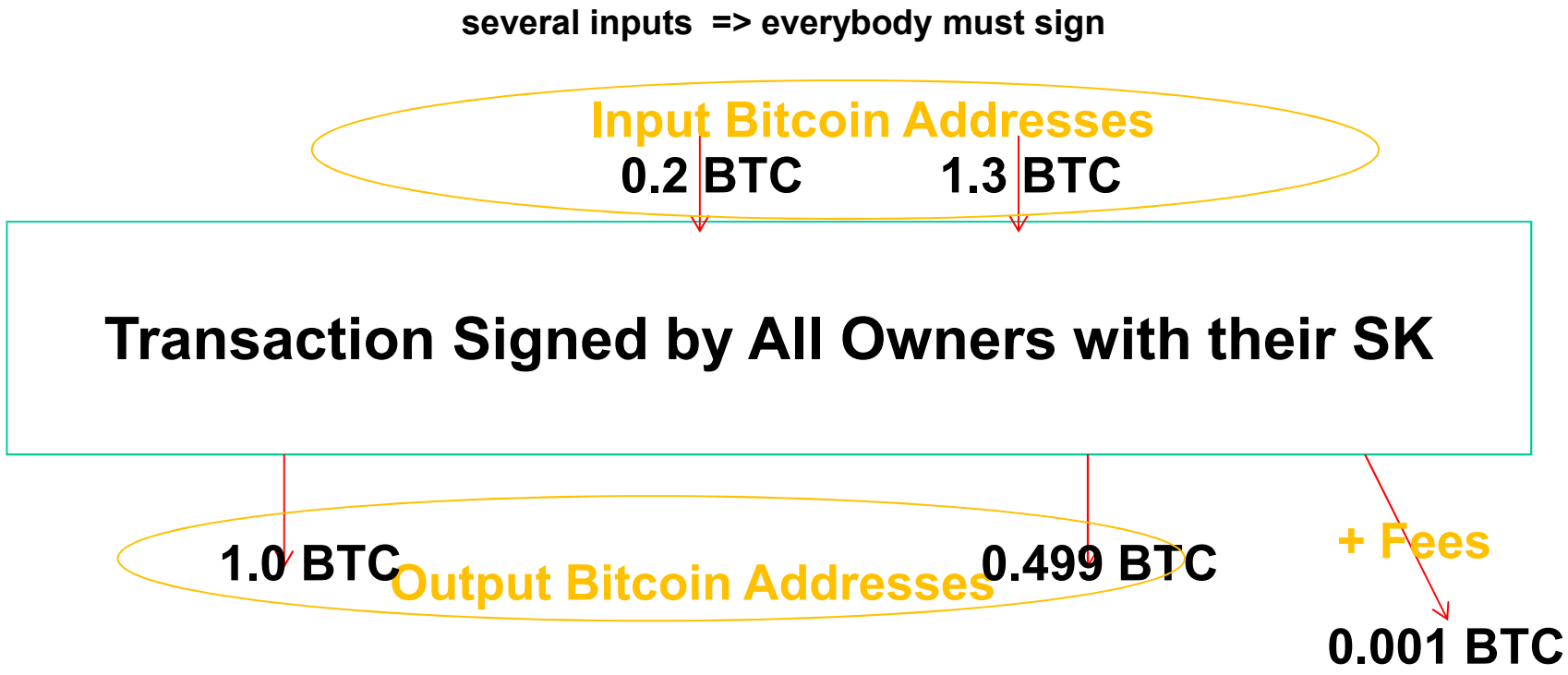
Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



Bitcoin Transfer

Transactions have multiple inputs and multiple outputs.



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


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

Bottom Line

Main Functionality:

-Private Key Generation

-Export public key

-ECDSA sign

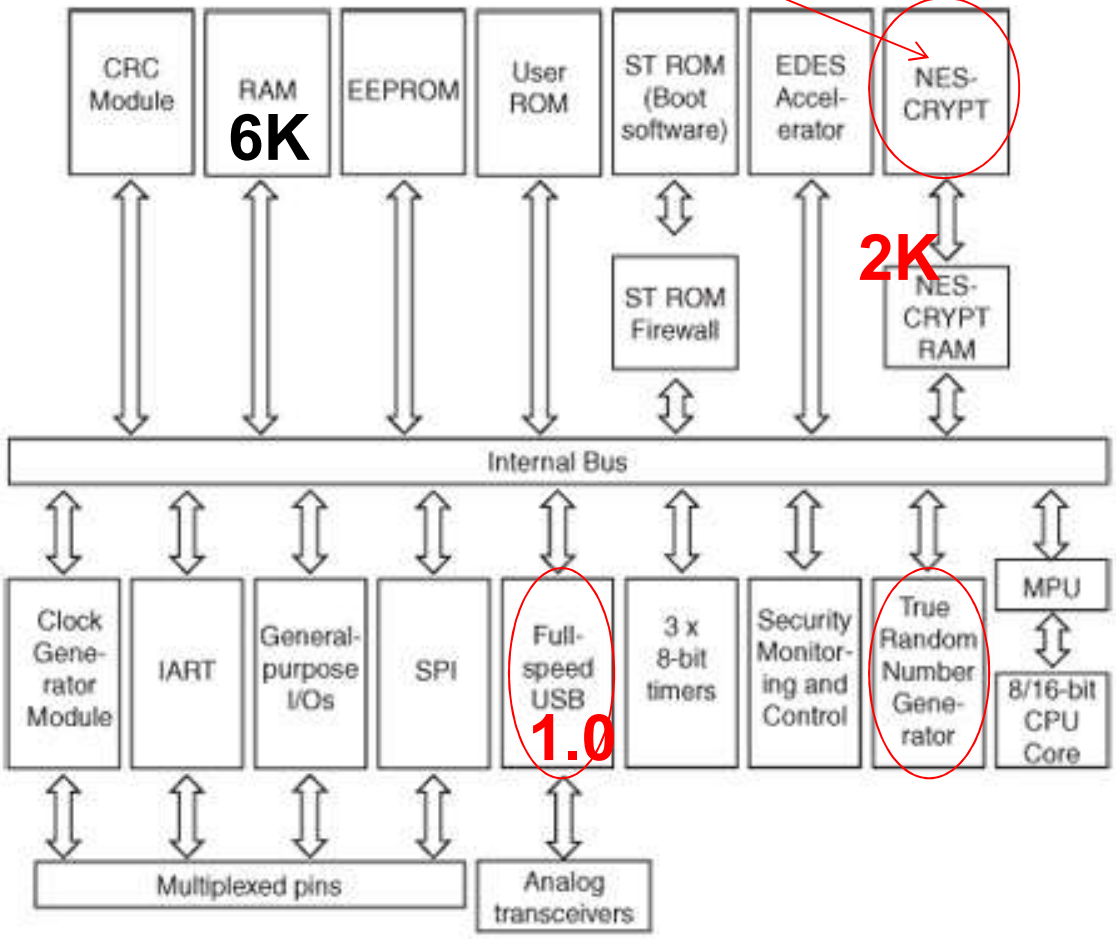
Ledger

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.

2. Least Common Mechanism

[Saltzer and Shroeder 1975]

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.

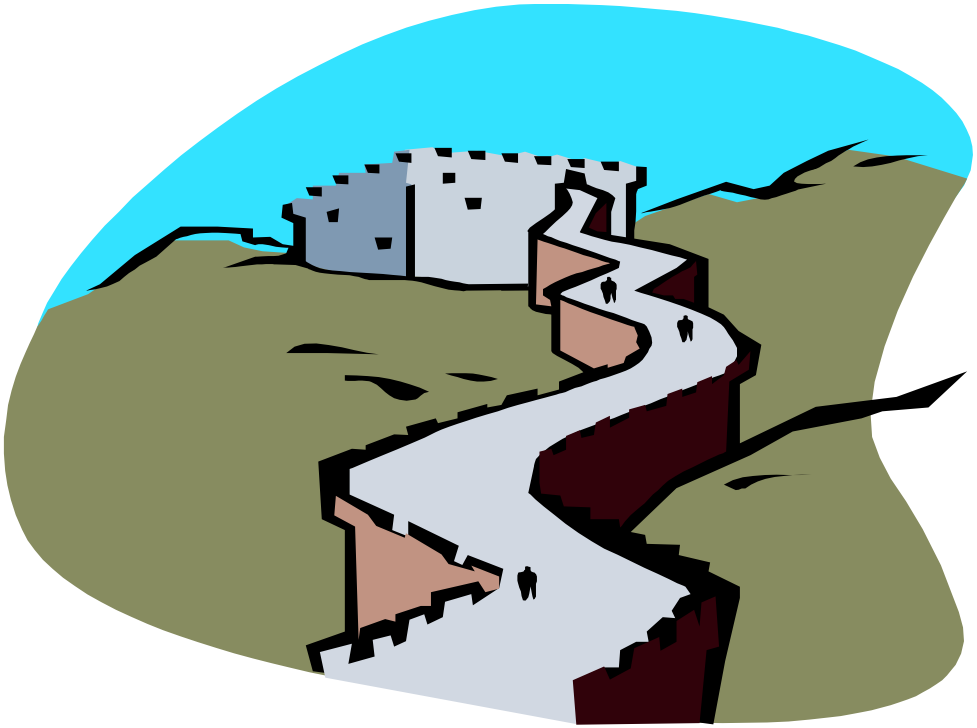
At minute 02.55: Dr. Nicolas Courtois of UCL:

"…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."

Hash Power => Security???

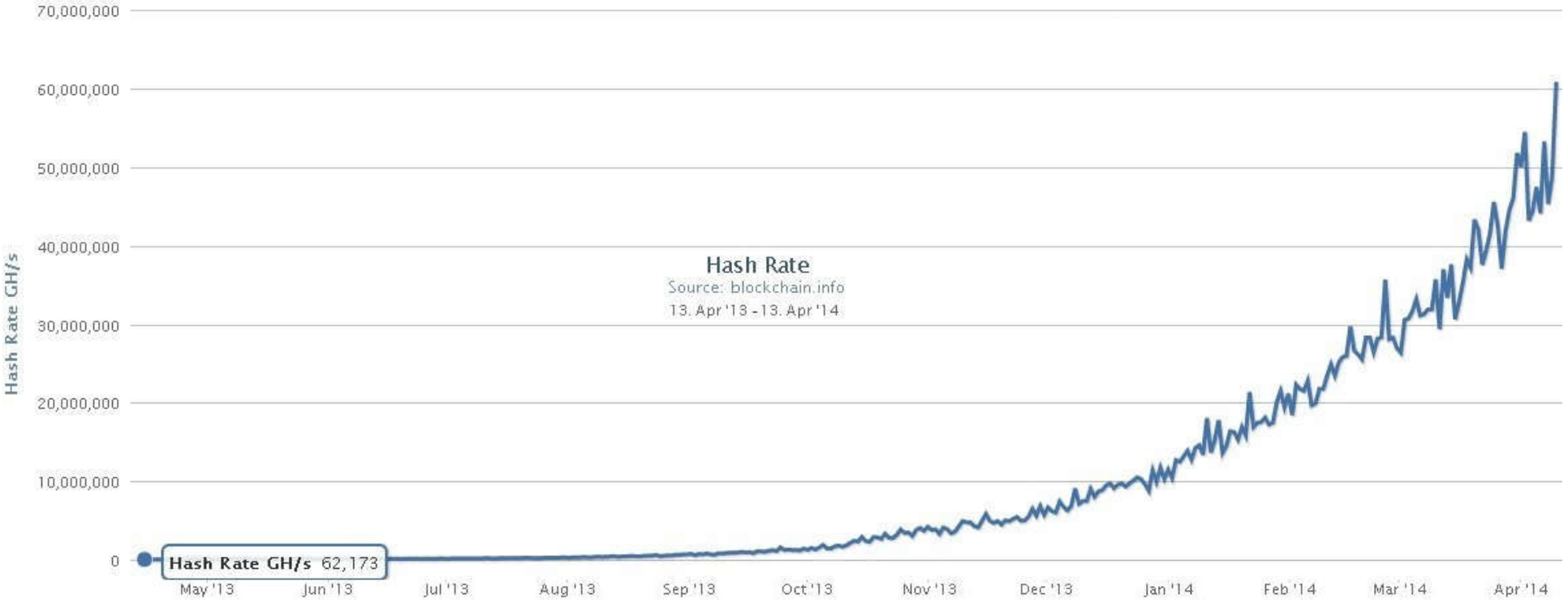
Sams writes: "The amount of capital collectively burned hashing fixes the capital outlay required of an attacker […] to have a meaningful chance of orchestrating a successful double-spend attack […]

REMARK:
THIS IS MISTAKEN!



Crazy Hash Power Increase

Nearly doubled every month… 1000x in 1 year.

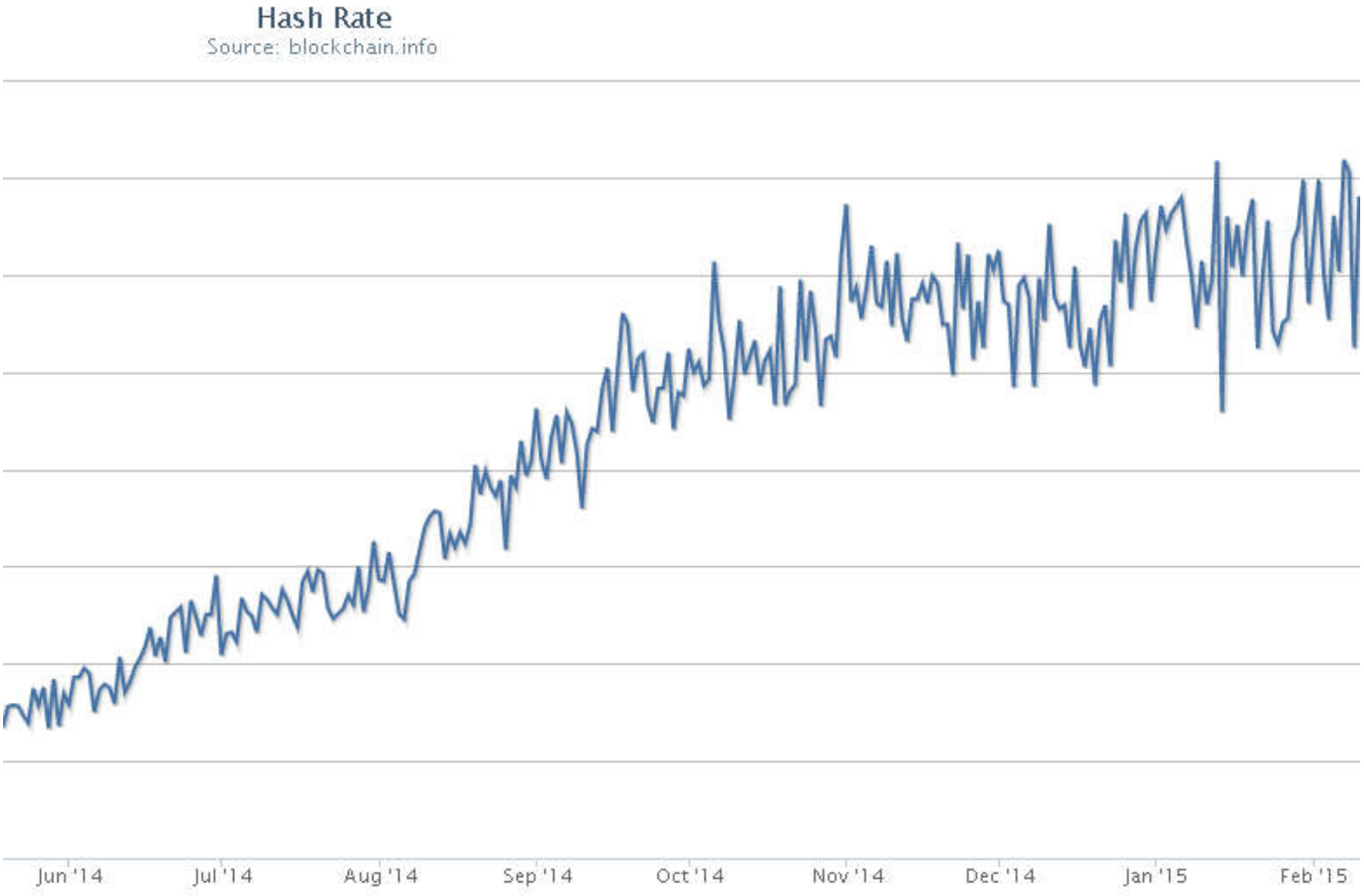


Thm:

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = 2$$

the total income is only **twice the income for the first month.**

Jan 2015: Plateau/Peak Reached



“Programmed Self-Destruction”

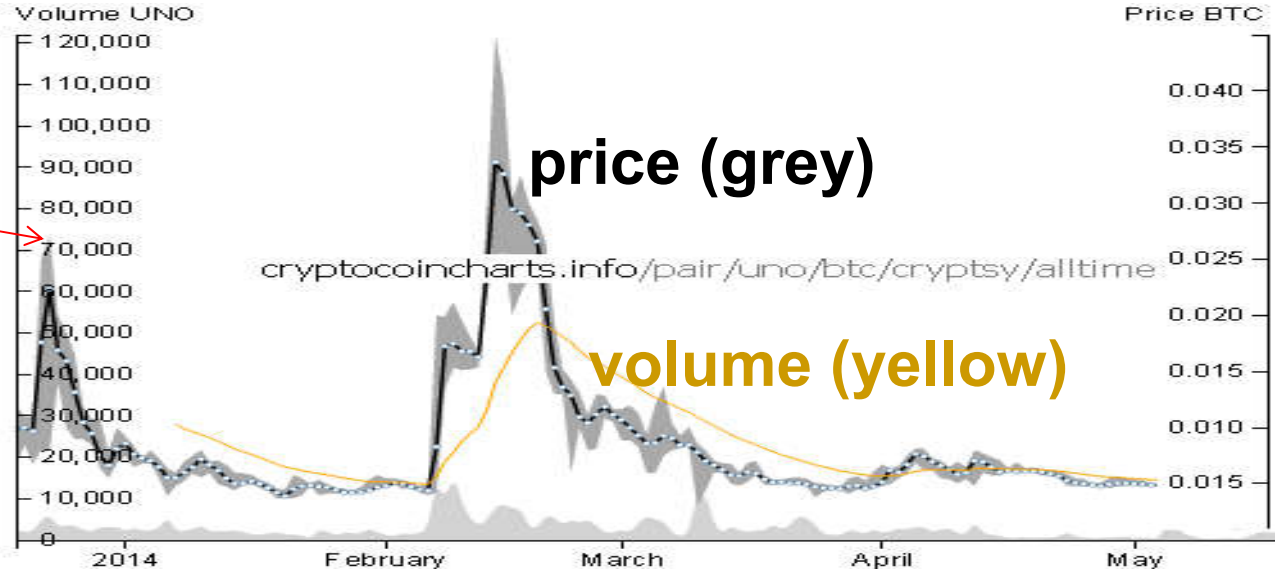
Nicolas Courtois: On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies http://arxiv.org/abs/1405.0534

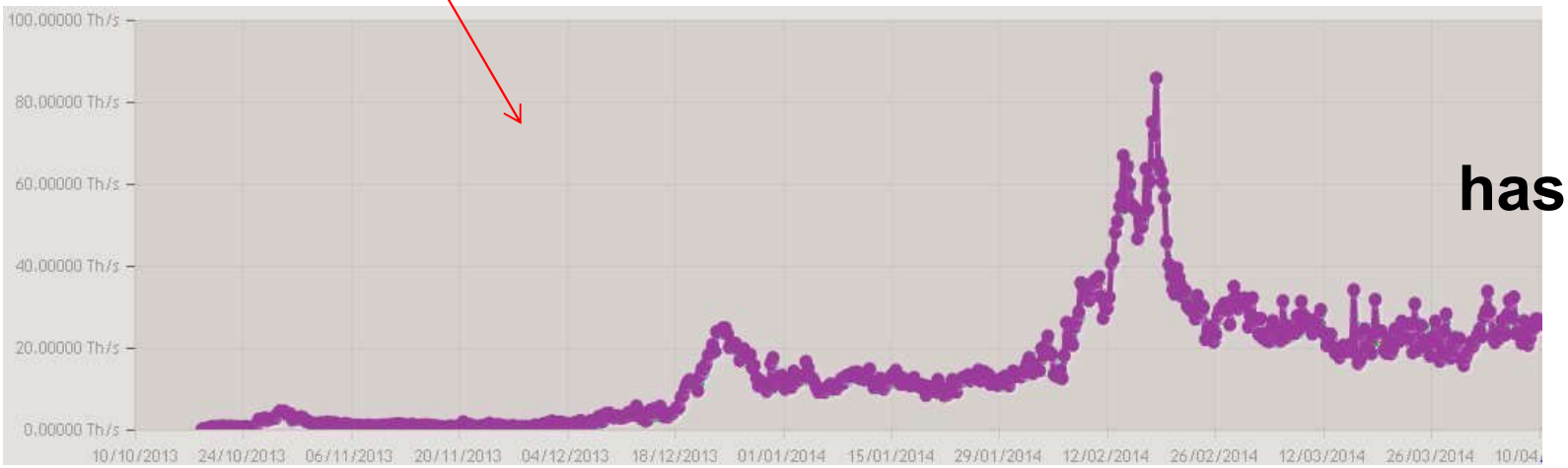
Unobtanium

– pump and dump: evidence

Cause:

Effect:





DogeCoin Predicted Decline [Courtois]

– hash rate MUST decline, as a result of monetary policy

Josh Mohland, 4 August 2014

Acknowledged that:

- Dogecoin was never "intended to function as a full-fledged transaction network",
- "Dogecoin was built to die quickly –none of us expected it to grow into the absurd entity it is today.
- With that said, there's absolutely an easy way to save the coin from its certain death (and by death I mean 51% attacked [...])"

=> after the reform Dogecoin Market price more than tripled…

Cryptome Renamed My Paper:

CRYPTOME

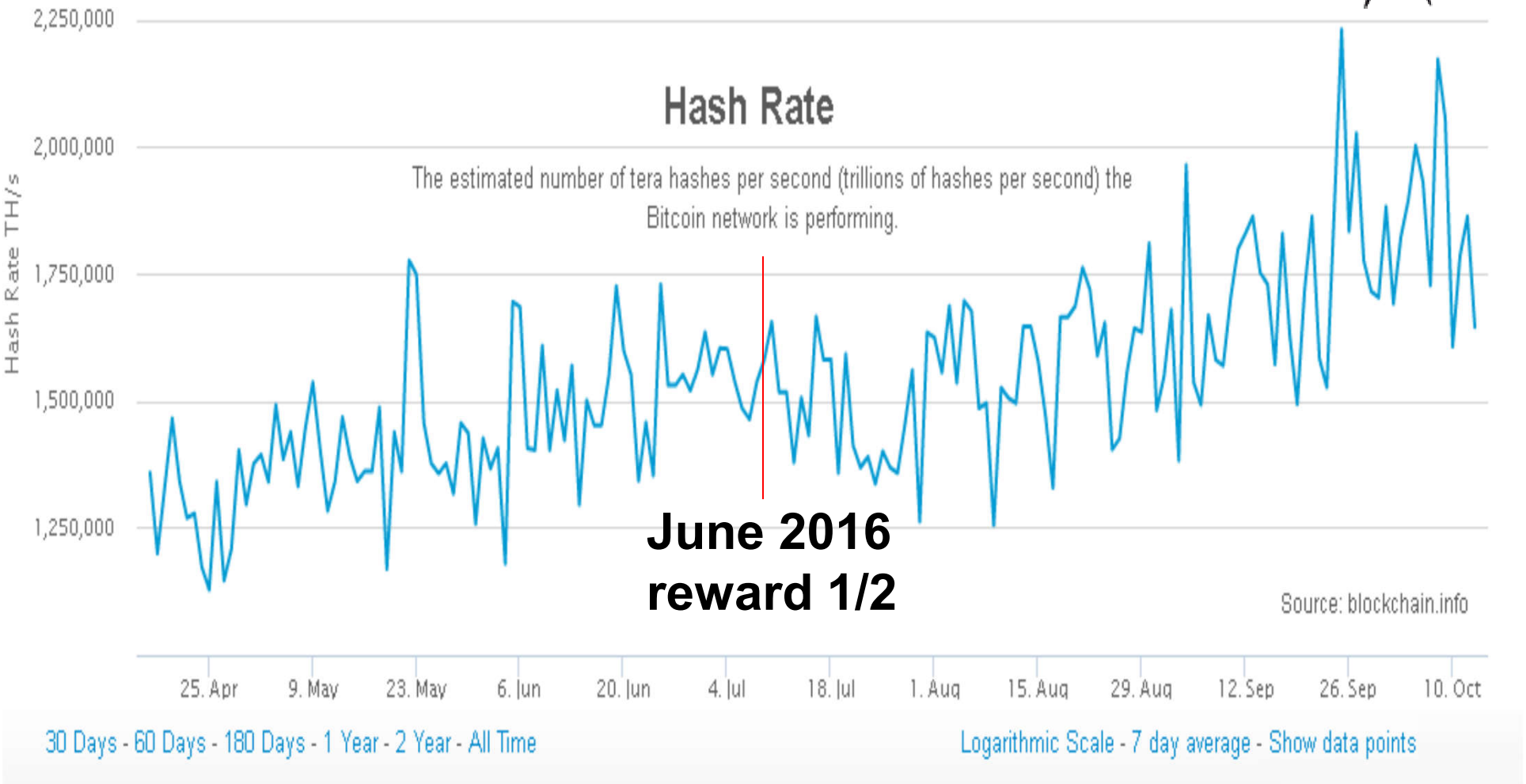
Donate for the Cryptome Archive of over 81,300 files from June 1996
key. (Local search temporarily disabled, use Google)
Bitcoin: 1P11b3Xkgagzex3fYusVcJ3ZTVsNwwnrBZ

http://cryptome.org/2014/05/bitcoin-suicide.pdf ?????????

=> Actually I show that quite possibly
bitcoin is EXEMPT from destruction [natural monopoly].

=> Whatever is Bad with bitcoin is
even worse with most alto-coins.

Bitcoin Hash Rate has NOT Declined



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!

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 [...]

- 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.

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

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)

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:	Ƀ 0.140
# of Bets:	3

Ƀ

PAYOUT	ROI
Ƀ 0.00	0%

*assumes current weight and volumes

Place Anonymously

NO	
Volume:	Ƀ 0.189
# of Bets:	6

Ƀ 0.1

PAYOUT	ROI
Ƀ 0.14327	43.27%

*assumes current weight and volumes

Place Anonymously