Introduction to Bitcoin

Nicolas T. Courtois

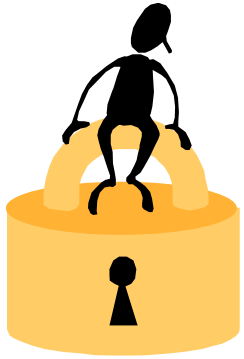
- **U**niversity **C**ollege **L**ondon, UK

“Cryptographer’s Dream”

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

Trust No One?

We still need to
trust the cryptography
(and cryptographers)



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

Disruption?

Disruptive Technology:

def:

Allows to do things which just could not be done before…

Bitcoin

Decentralized peer to peer payment system which works as currency:

=> has units of value which can be exchanged for “real money”. Currently 1BTC= 300 GBP

Based on cryptography and network effects.

Anarchy, not supported by any government and not issued by any bank.

Are They Crazy?

Anything can be “money”
if sufficiently many people accept it… (e.g. salt).

Question of:

- popularity

  legal tender, government standardization and regulation

  <= in Google searches and press/media

  bitcoin is a lot more famous than Snowden/NSA etc…

- trust

  trustworthy authority

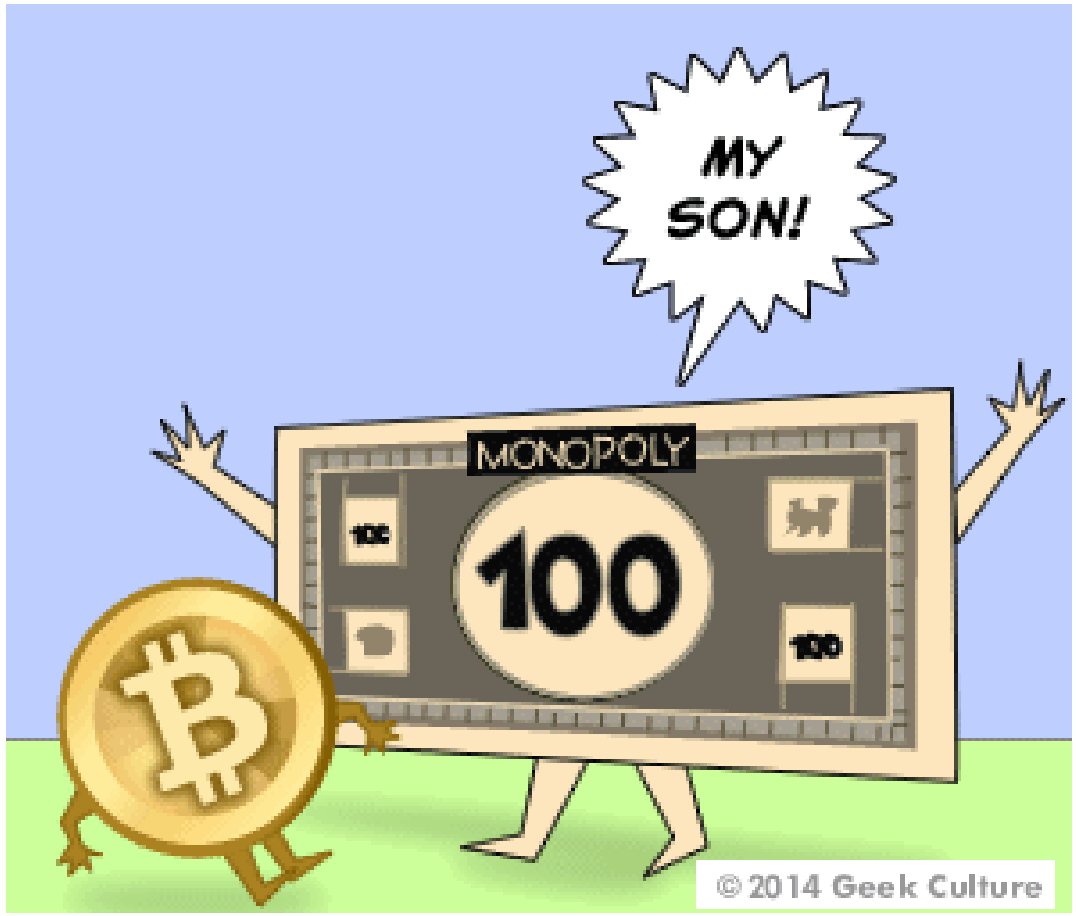
  <= distributed computer system

  acting on self-interest

  NO NEED TO TRUST ANYONE

Play Money?

A distinction play vs. real money has almost disappeared recently.

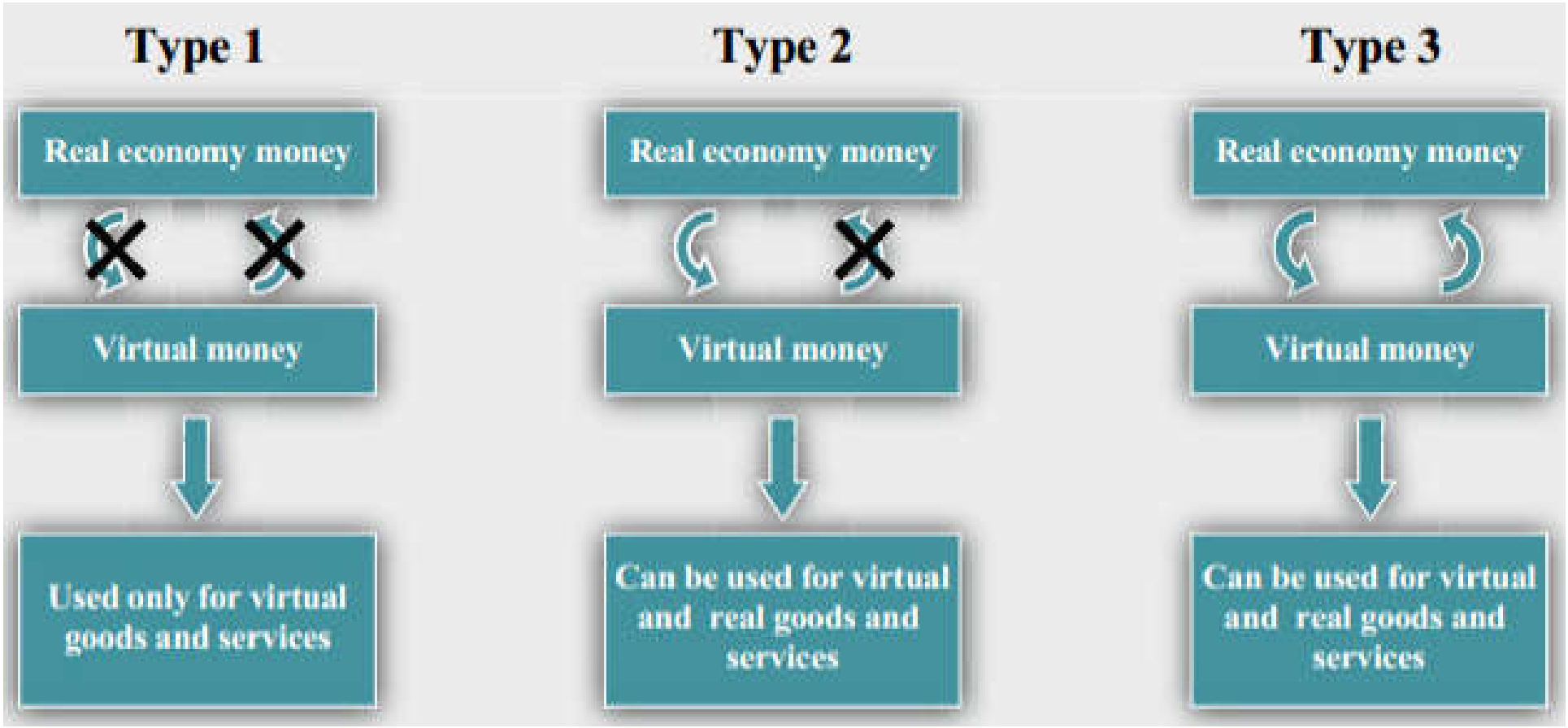


Types of “Virtual Money”

Source: ECB report, 10/2012

http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

cf. Oyster…



Freedom

Hegel [1770-1831], German philosophy

The history
is the process
of broadening
freedom.

9 Nov 1989 Berlin Wall Has Fallen

In Eastern Germany

You had a typewriter,
or a photocopier,

⇒You were the enemy
of the government!

Stasi secret police officers interviewed travellers entering or leaving East Germany in this room at the Marienborn border crossing point

Today

- anyone can have a blog.

20th Century

- anyone could have a blog…

UCL Bitcoin Events

21st Century:

- anyone could have a blog…

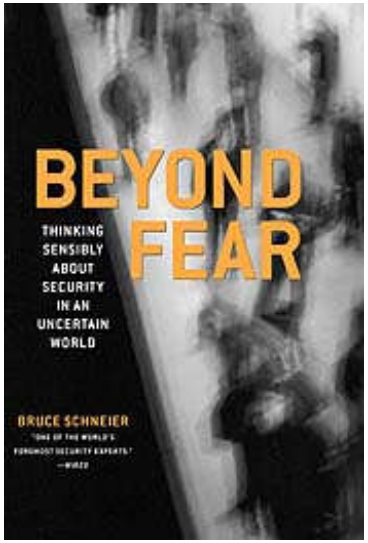
- anyone can print his own currency!

Ban Bitcoin?

Ban Bitcoin?

- There is no “undo” button for sth. like bitcoin [Mike Gogulski]

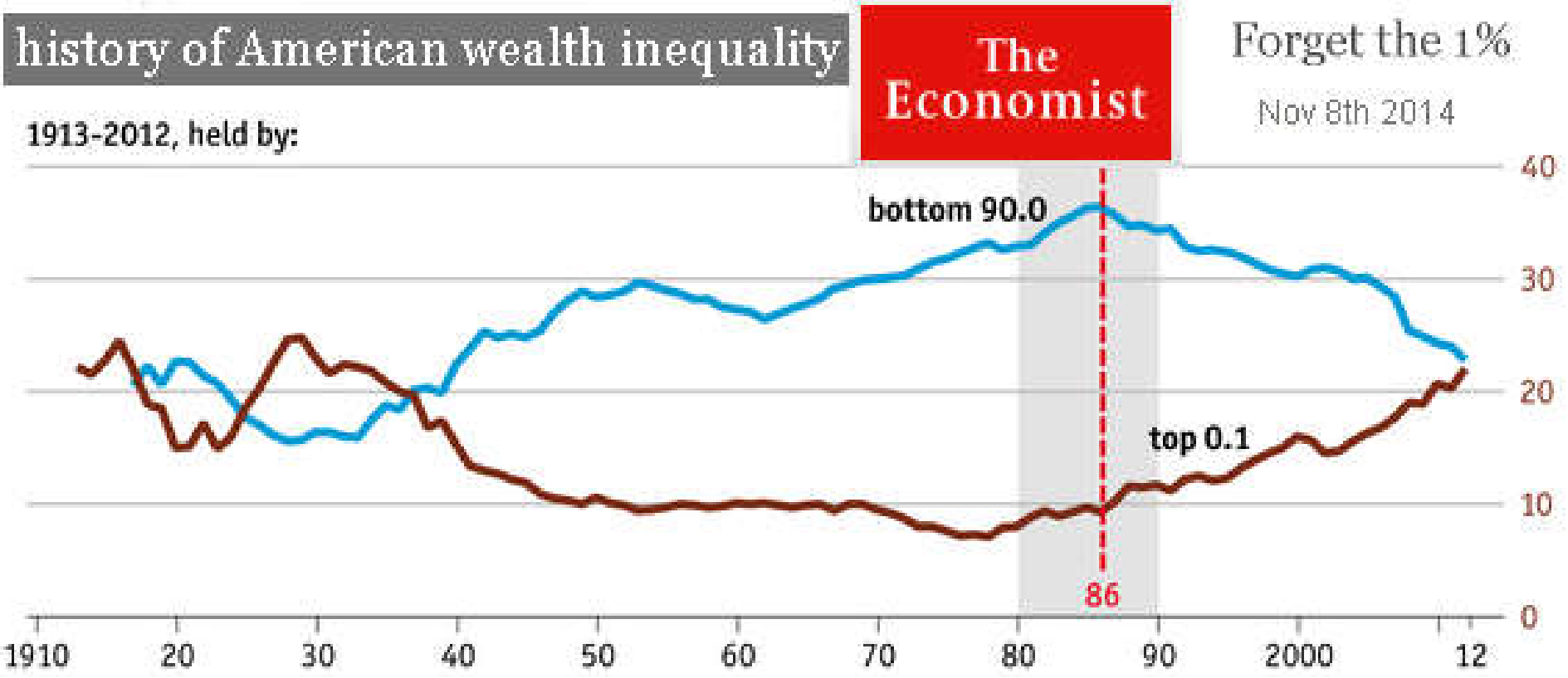
Freedom vs. Security



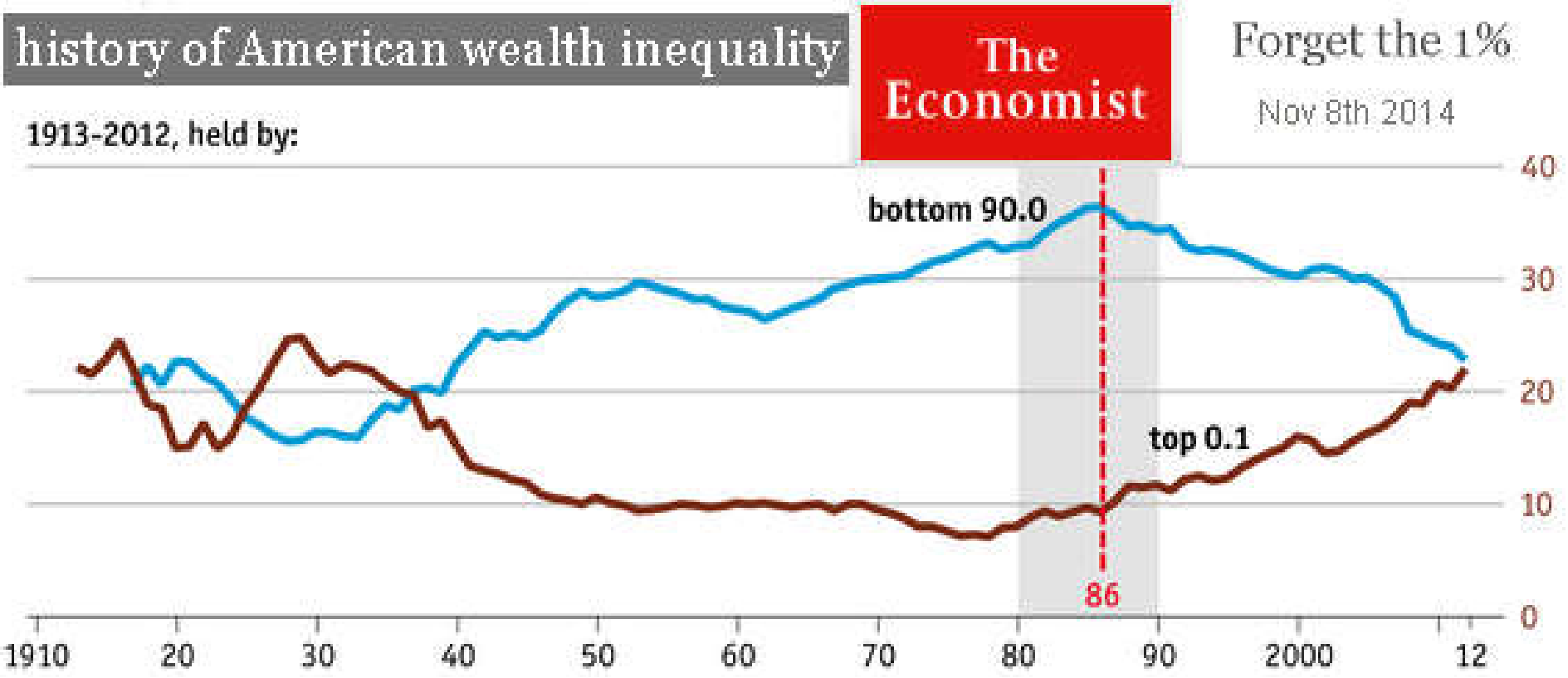
We failed to protect our DATA

We failed to protect our MONEY

In the Last 25 years Freedoms Have Declined!

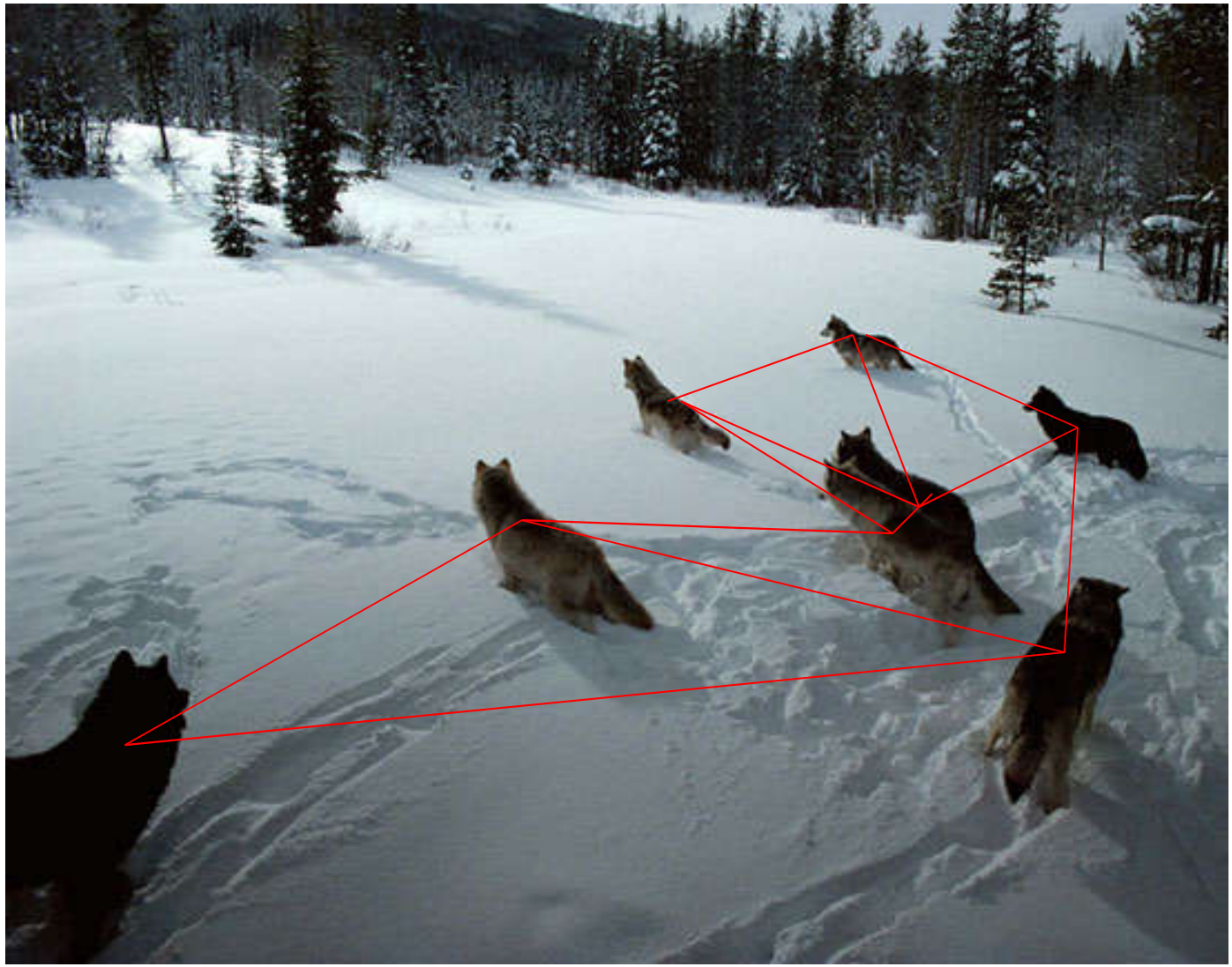


In the Last 25 years Freedoms Have Declined!



Physical Oppression => Financial Oppression

Solution = Decentralization



Miracle Of Bitcoin

Removes two pillars of money:

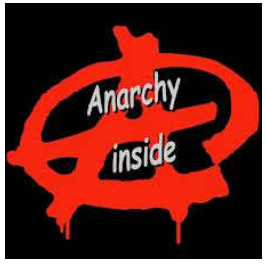
- "trust"

  => Peer 2 Peer self-regulation

  based on self-interest?

- legal/government protection and policing

  => anarchy!



Decentralized P2P Finance

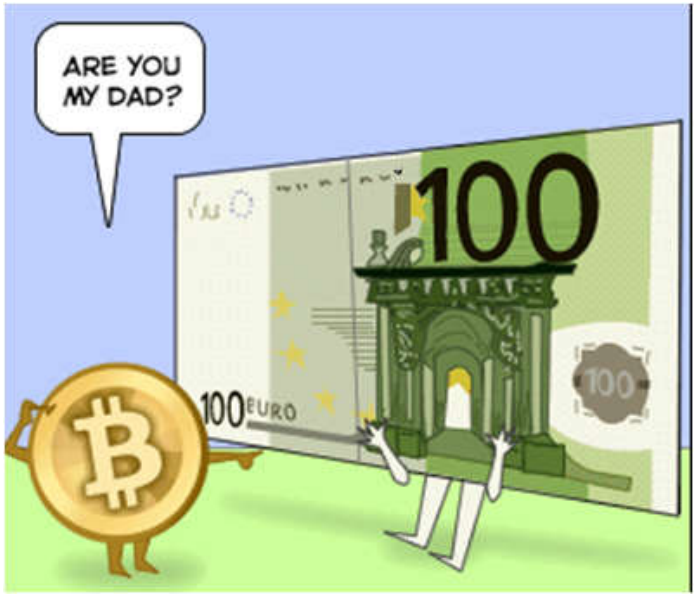
- Until recently, we've needed central bodies – banks, stock markets, governments, police forces – to settle vital questions.
  - Who owns this money?
  - Who controls this company?
  - Who has the right to vote in this election?
- Now we have a small piece of pure, incorruptible mathematics enshrined 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

Bitcoin vs. Money



Money

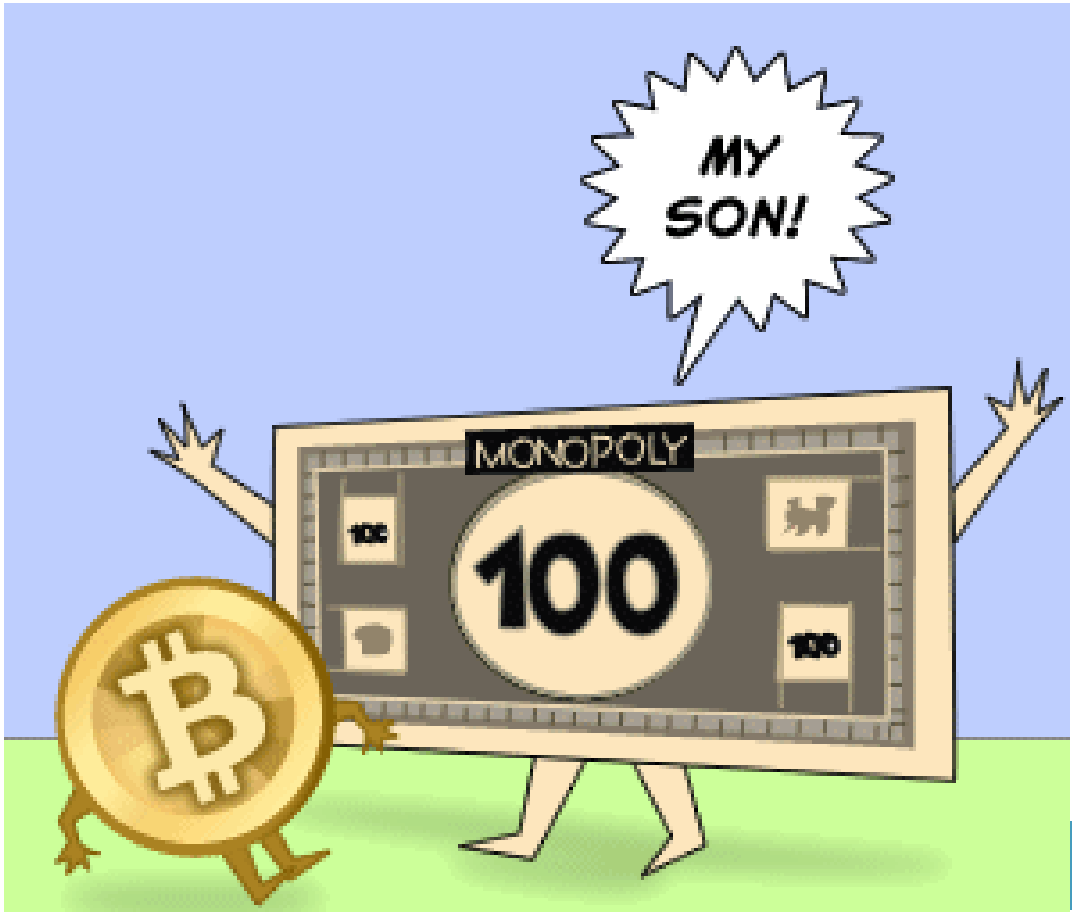
Key invention
in human history:

money

- here is some money for your research

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

Bitcoin

Based on cryptography and network effects.

Private money.

Is Bitcoin Money?

- We will NOT claim it has all the characteristics of money.
  - it definitely has some!
  - they are traded against traditional currencies at a number of exchanges.
  - bitcoins are “legal” by default,
  - not regulated by governments yet

3 Main Functions of Money

1. Store Value
2. Allow Payment
3. Unit of Account

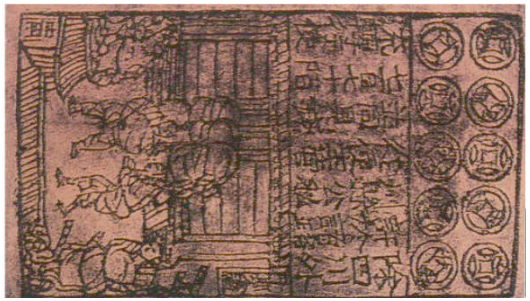
“Fiat Money”

Def:

Government-issued money not convertible for anything particular

(E.g; gold, goods etc).

paper money: introduced during Song dynasty, 11th century, China



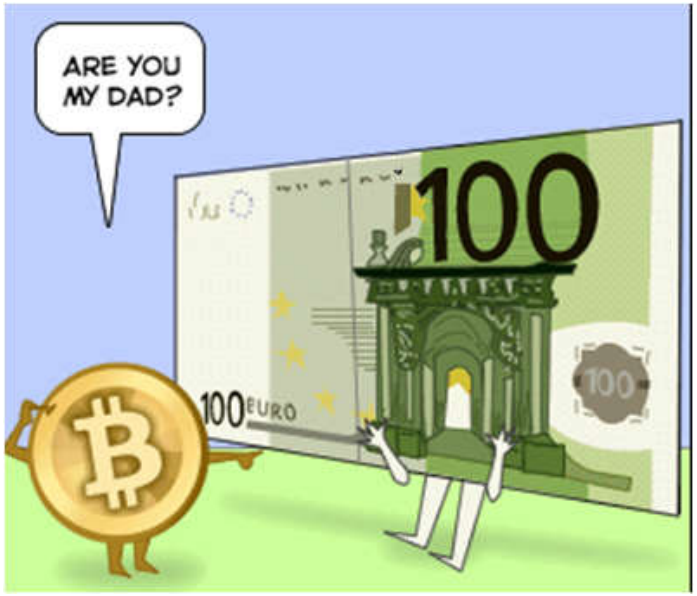
Bitcoin is…

"a low-cost replacement for credit cards and other payment mechanisms"

Very close to the business of

- Western Union
- CurrencyFair
- PayPal
- Mastercard/VISA
- Etc…

Bitcoin



Bitcoin

Bitcoins are cryptographic money

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

PK A

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

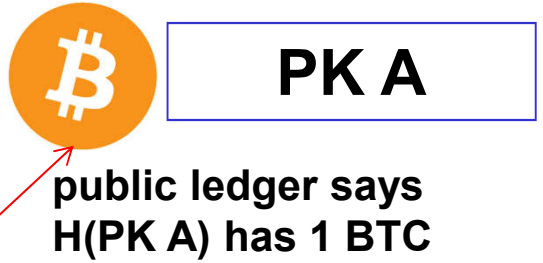
- to earn bitcoins one has to “work” (hashing) and consume energy (pay for electricity)
- do a difficult computation => you have earned 25 bitcoins
- works like a lottery (1 winner/10 minutes)

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

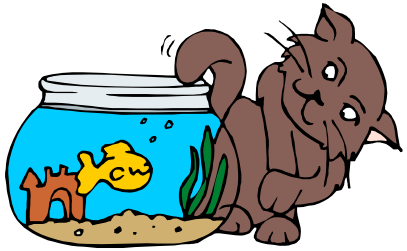
- to earn bitcoins one has to “work” (hashing) and consume energy (pay for electricity)
- do a difficult computation => you have earned 25 bitcoins
- works like a lottery (1 winner/10 minutes)



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

Authorizing Transfer of Coins

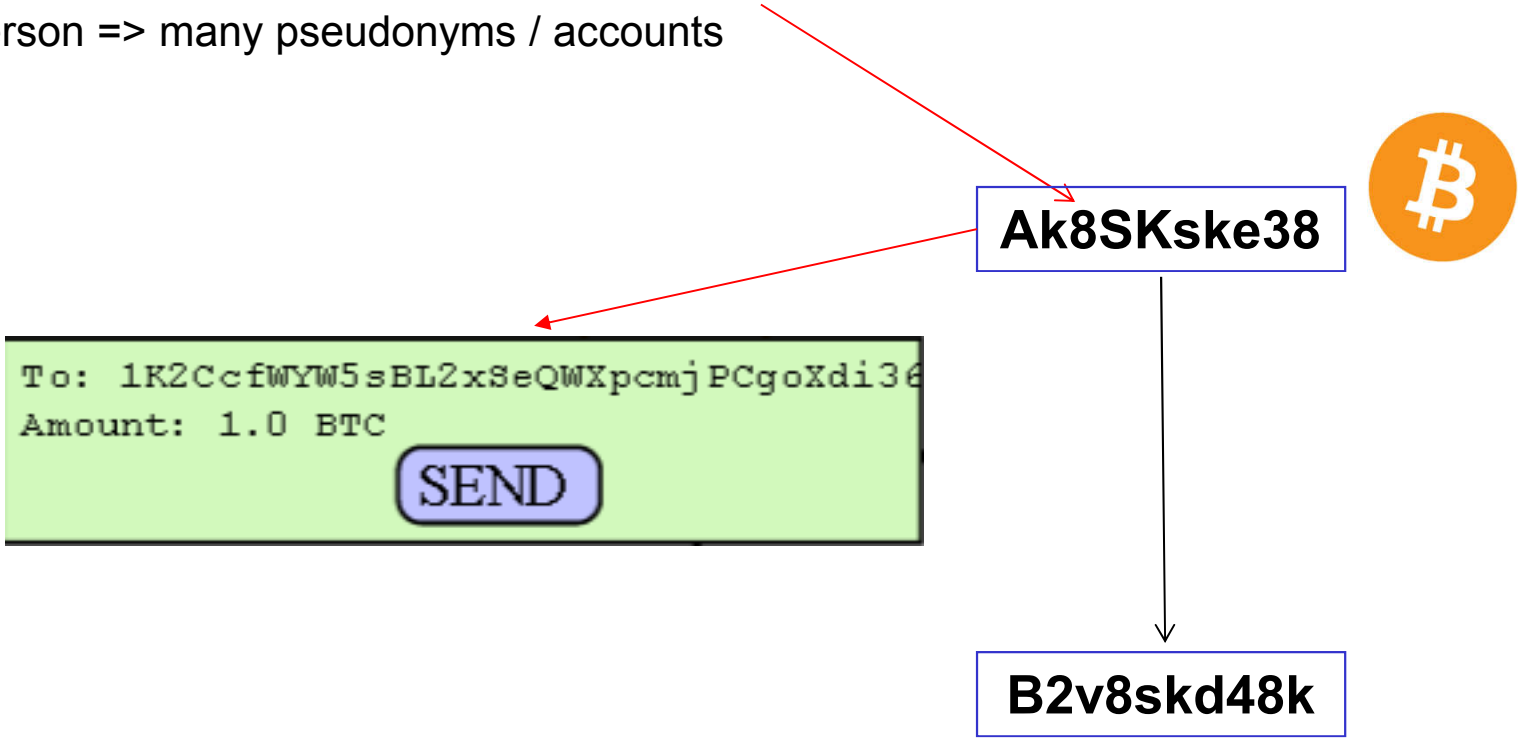
- you have a private key => you have the money (right to transfer)
  - money stored on PCs or mobile phones?



  - better solution: smart card

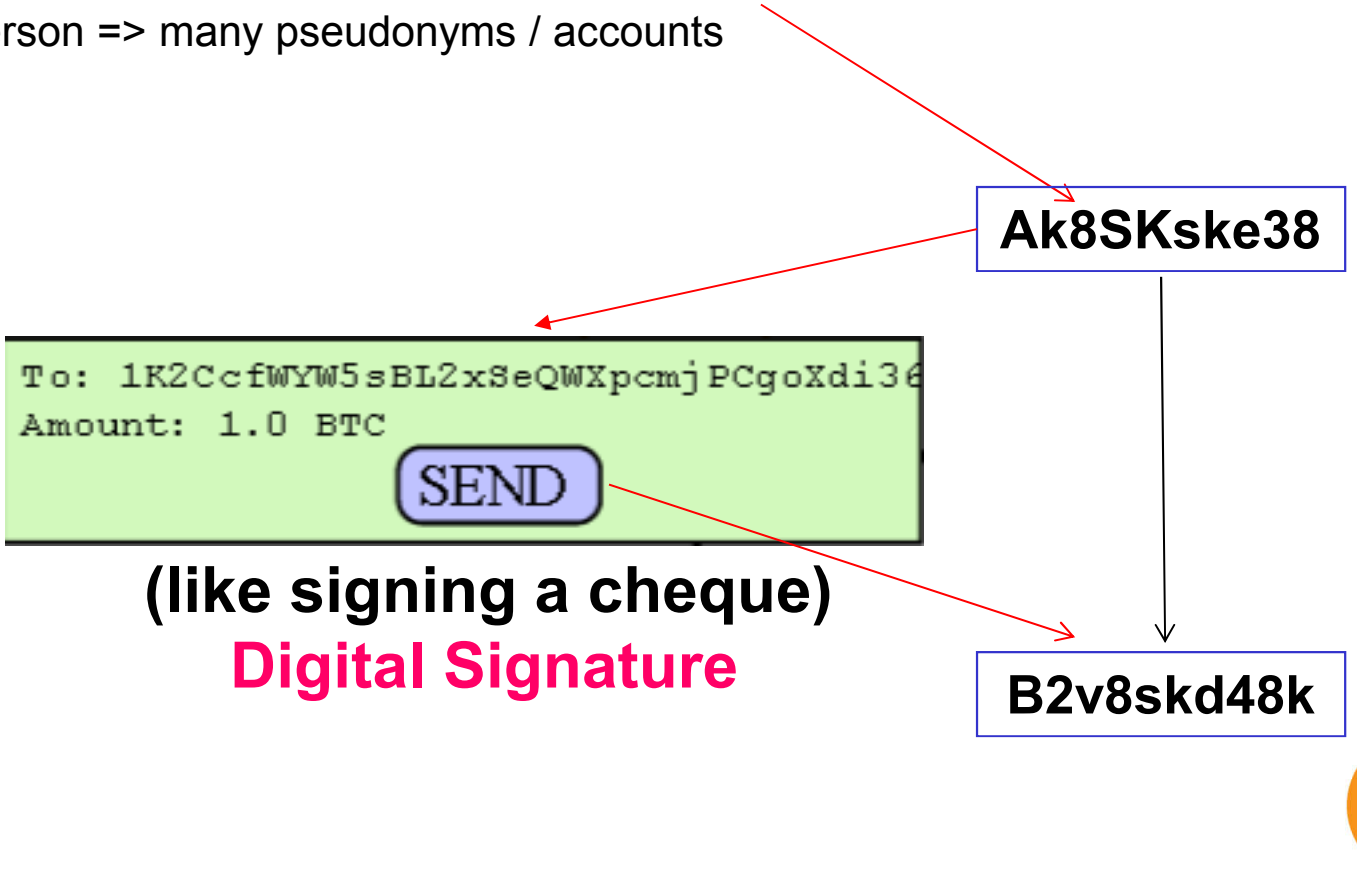
Bitcoins

- 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



Trust Less!

Digital Signatures ENABLE
these TRUSTLESS systems!

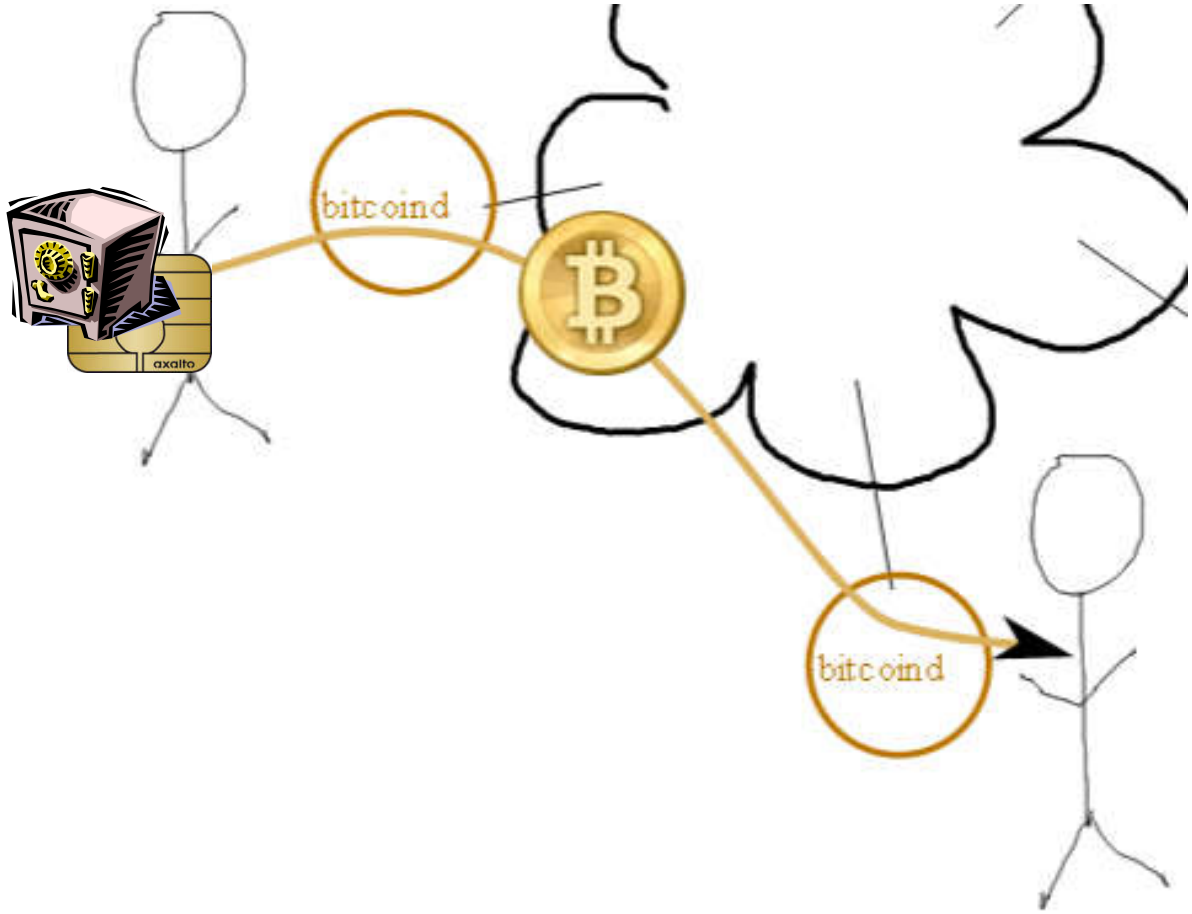
Example: My bank card signs a transaction with RSA, the bank does NOT know the private key,
ONLY the public key.

⇒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



Digital Signatures

Attaching a Signature

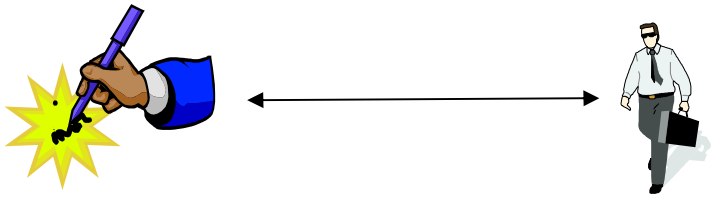
Signature – def:

data in electronic form which are attached to …
other electronic data
and which serve as a method of authentication.

Signatures

Two main functions

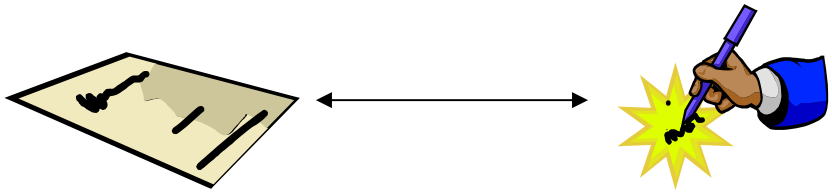
1. Identify the signer



Signatures

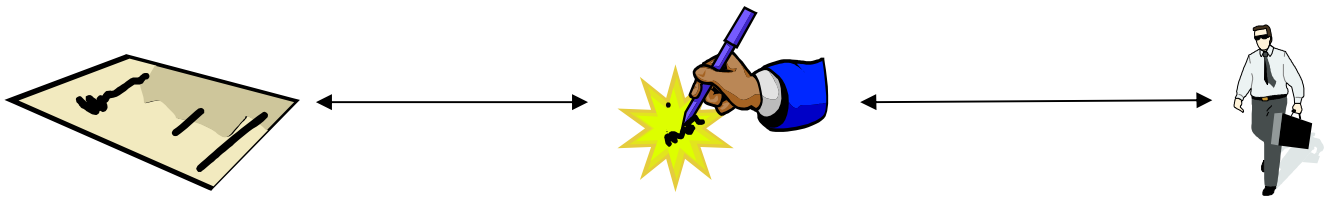
Two main functions

1. Identify the signer
2. Approbation



2x Link

- EU Directive 1999,
- UK Electronic Communications Act 2000



Digital Signatures

Three main functions now:

1. Identify the signer
2. Approbation
3. Integrity of the message

   (cannot be modified later)

Solutions: Digital Signatures

Idea: cryptographic solution

Definition: 3 algorithms…

key generation algorithm

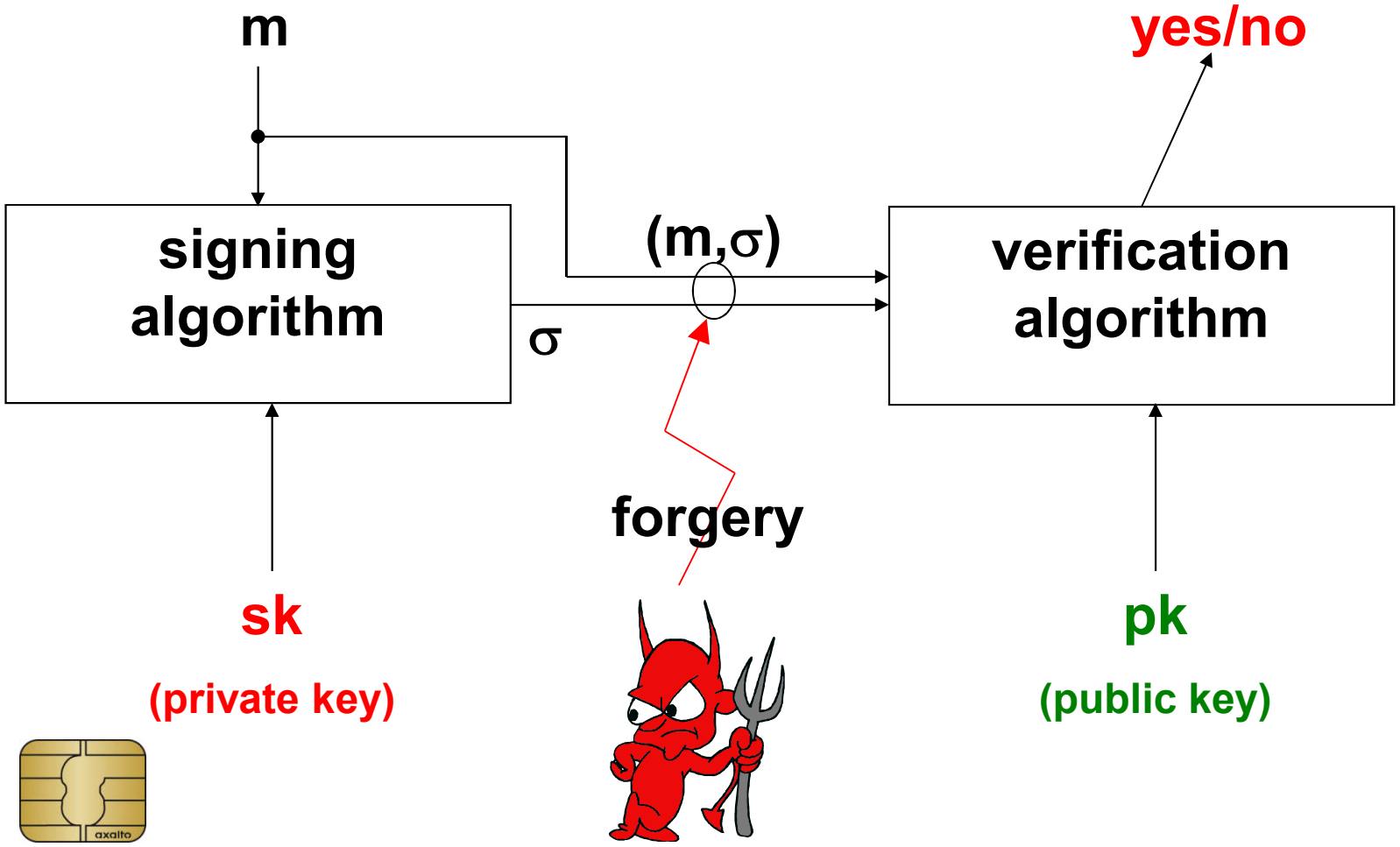
sk

(private key)

pk

(public key)

Digital Signature

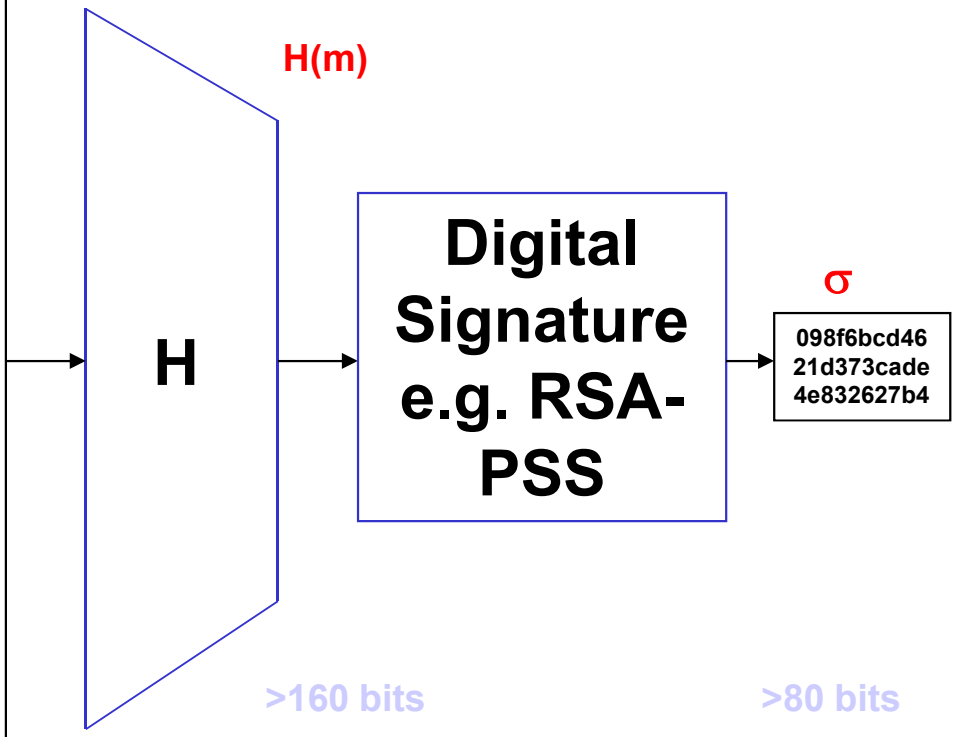


Hash-then-Sign

m

A hash function (or hash algorithm) is a reproducible method of turning data (usually a message or a file) into a number suitable to be handled by a computer. These functions provide a way of creating a small digital "fingerprint" from any kind of data. The function chops and mixes (i.e., substitutes or transposes) the data to create the fingerprint, often called a hash value. The hash value is commonly represented as a short string of random-looking letters and numbers (Binary data written in hexadecimal notation).

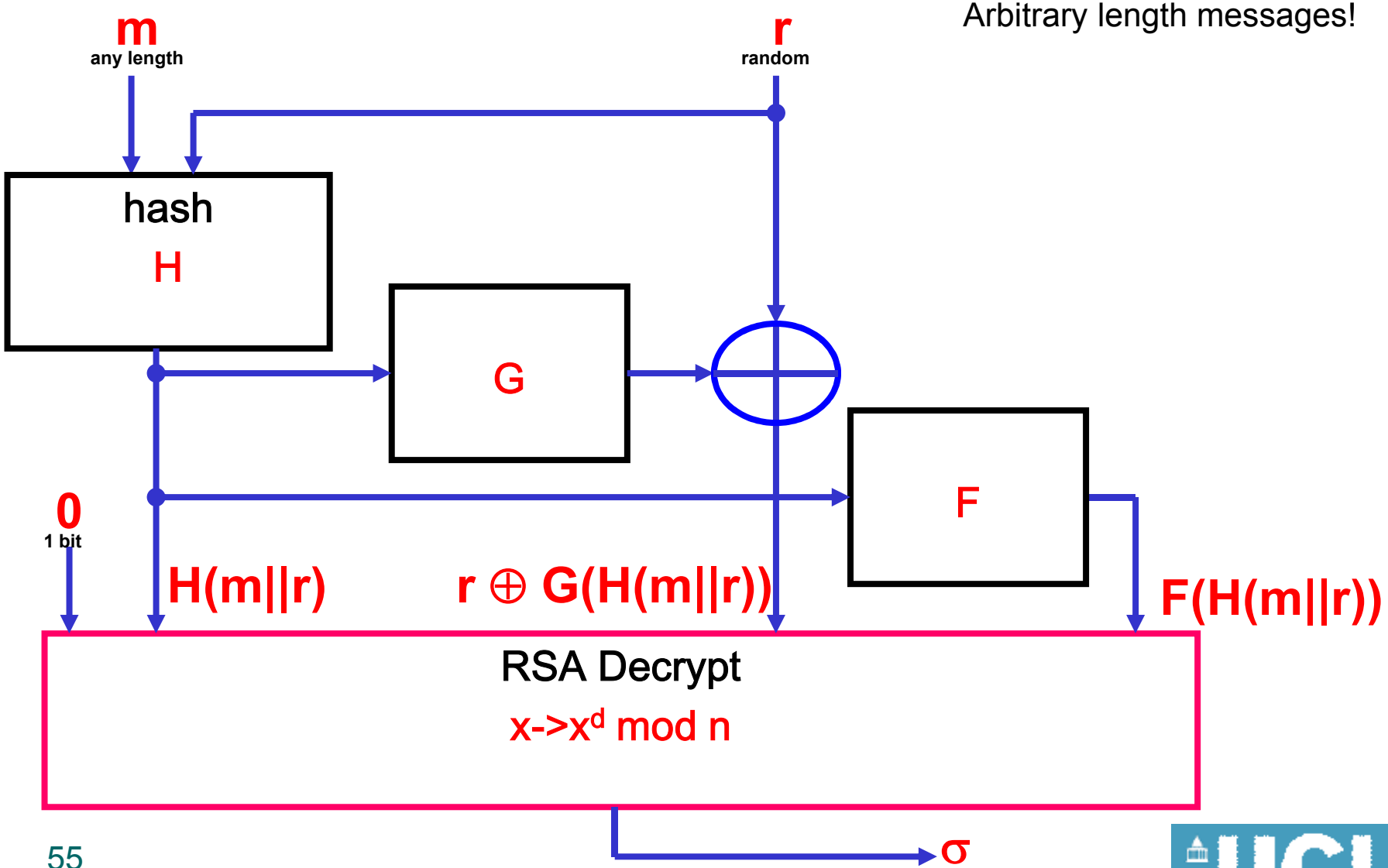
0-∞ bits



Probabilistic Signature Scheme [Bellare-Rogaway'96]

Uses a hash function H and two one-way functions F and G.

Arbitrary length messages!



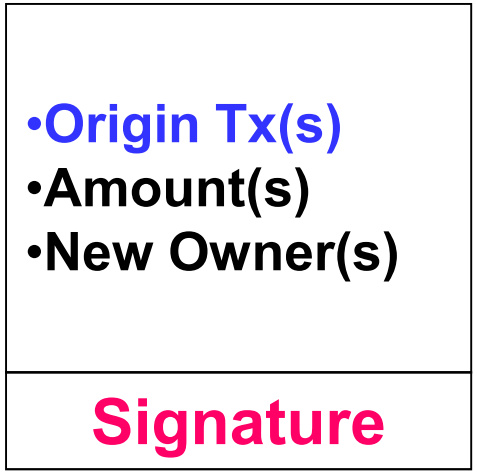
Digital Signatures - Bonus

Another main function !

4. Automatic verification,
   and better:
   Public Verifiability
   (anyone can verify!)

Authorizing Transfer of Bitcoins

- you have a private key => you have the money (right to transfer)
  - keys stored on PCs or mobile phones
  - publicly verifiable, only one entity can sign
- you can transfer ALL yet unspent attributions
- if Tx has several inputs
  => everybody must sign
- data to be signed:



Tx LifeCycle

- Miner nodes

tx

- Peer Nodes

tx

- Wallet Nodes

burn

public ledger

Blockchain

Block Chain

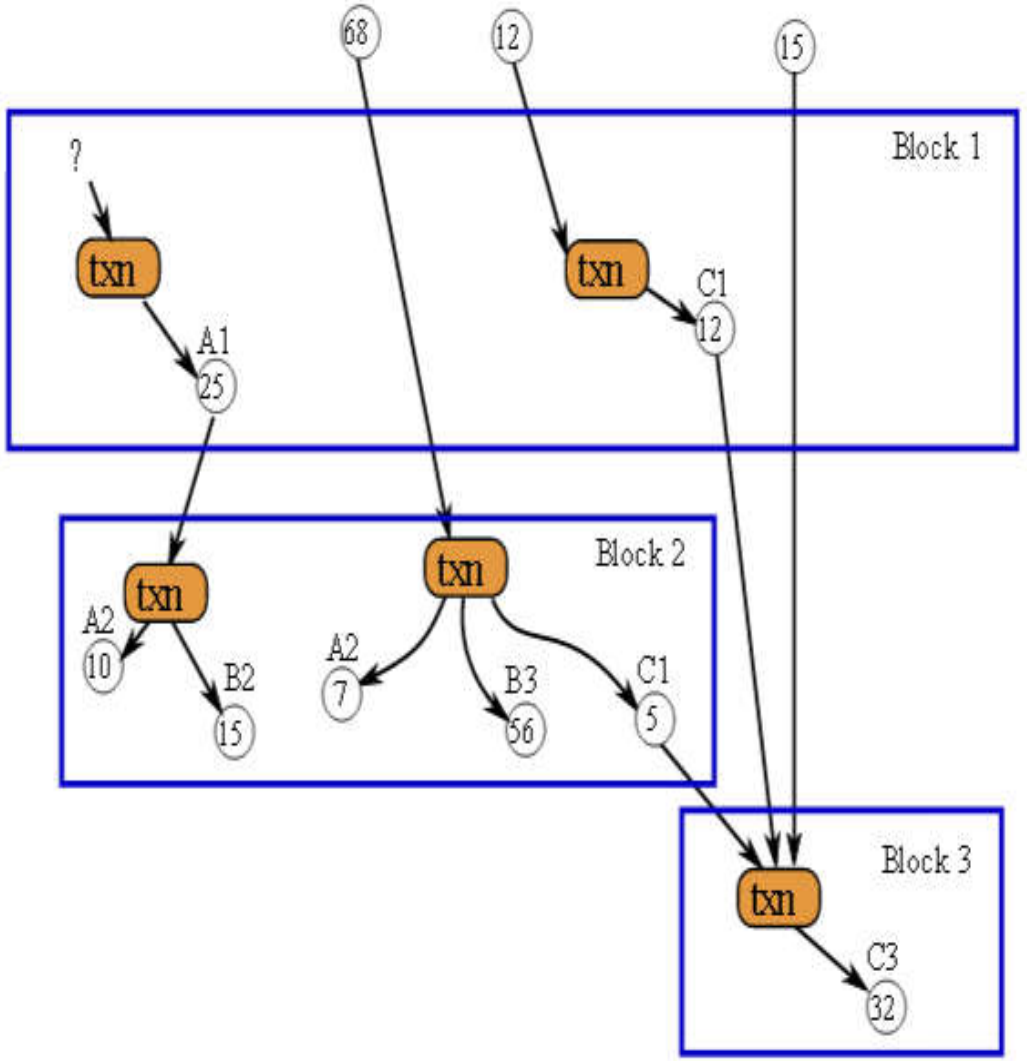
Def:

Public transaction database
or a ledger.

Every transaction
since ever is public.

Blocks contain a
Proof Of Work (POW)

(they are basically
hard to make)



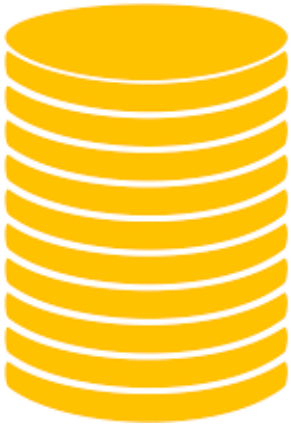
Multiple Confirmations

=>each new block confirms
ALL previous events

<u>Security:</u>

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

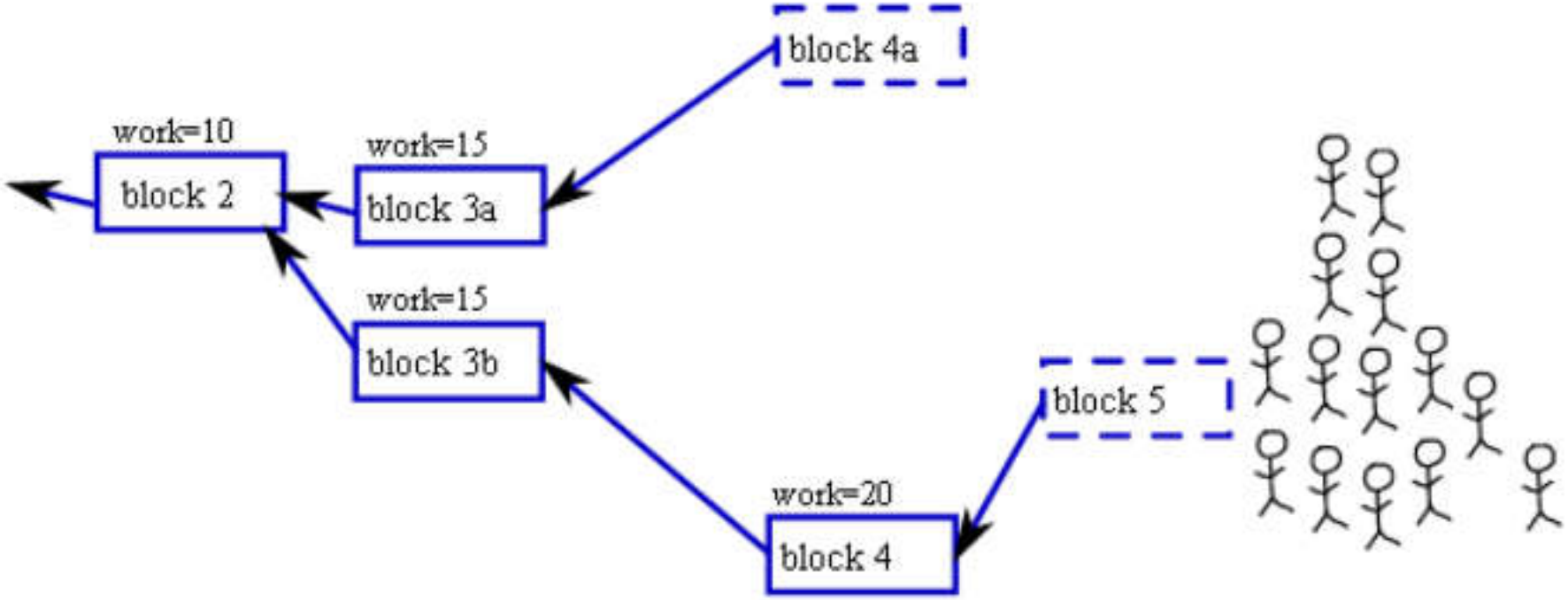
- evidence piles up
- with time it becomes too costly to cheat

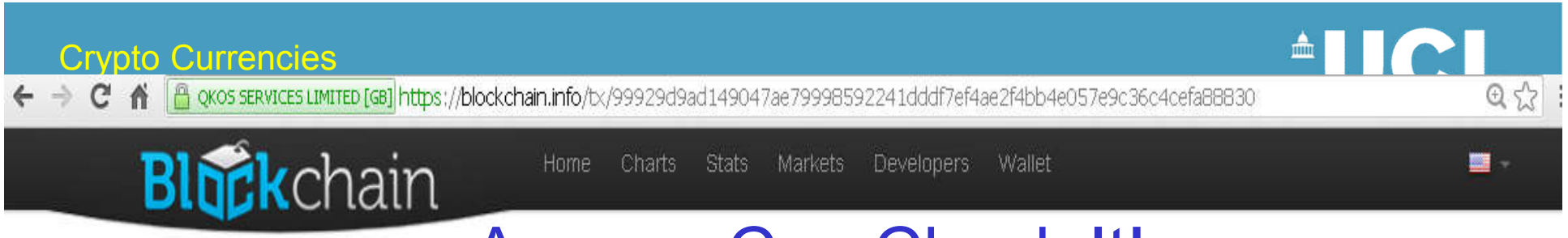


Stability - Longest Chain Rule

[criticised in our research]

"1 ASIC 1 vote"





Anyone Can Check It!

Transaction View information about a bitcoin transaction

99929d9ad149047ae79998592241dddf7ef4ae2f4bb4e057e9c36c4cefa88830

unique ID on 256 bits = the hash of the whole

1EWJJCnBuyQDPwVHuCycUCMHCVxTSGLBvk
1MisJY7KwjnhmdaMwyH6v1A3jDQpty7rdg

multiple inputs
tx origin + index of each is

1BaQzo1SyRXZRhQwSvsQJKAUvi5tu3L9uQ 10 mBTC
1rpU1Wa3pYeuJEbRPMWDDCxeh5PDMBrQ9 83.50001 mBTC
1BSy1ARBQfT9PRDYYB6DvzRkbSVRrgbaX3 1.39661 mBTC

Multiple recipients

94.89662 mBTC

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

Functional Separation

There are 3 distinct groups of people:

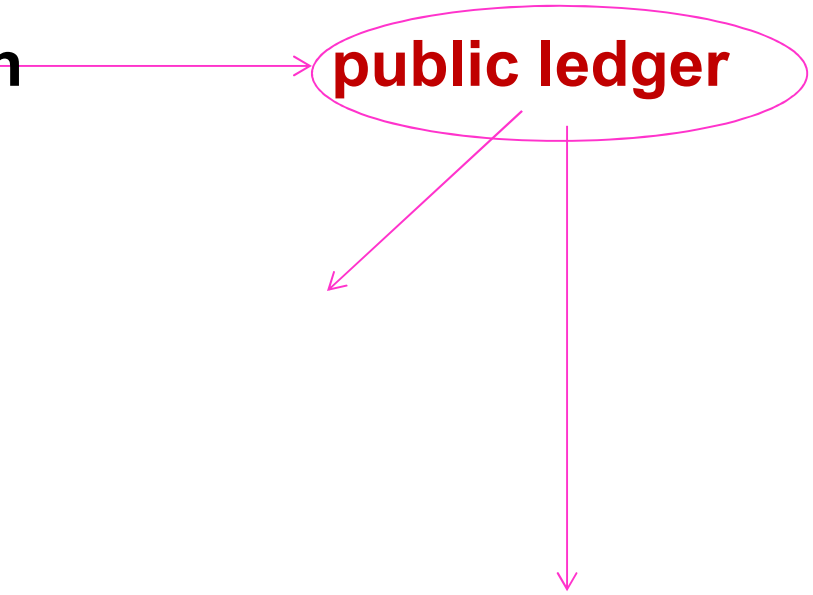
- Miner nodes – 50K
  - Hashing with public keys
- Peer Nodes – 5K
  - Relay and store transactions and blocks
- Wallet Nodes – 5.5M, 0.25M active
  - Store and release funds,
  - Focus on management of private keys, master keys etc etc.

Tx LifeCycle

- Miner nodes
- Peer Nodes
- Wallet Nodes:

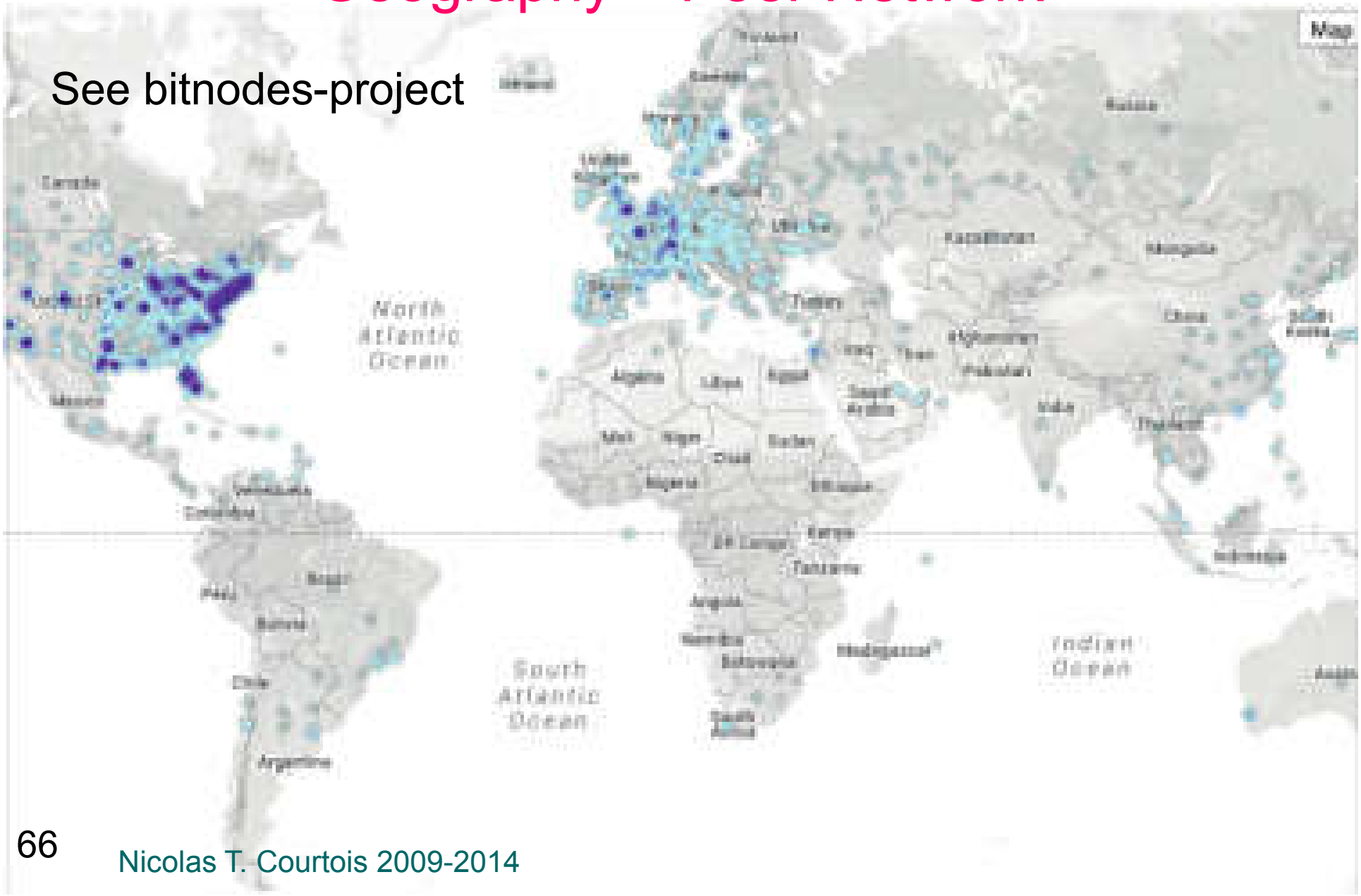
tx

tx



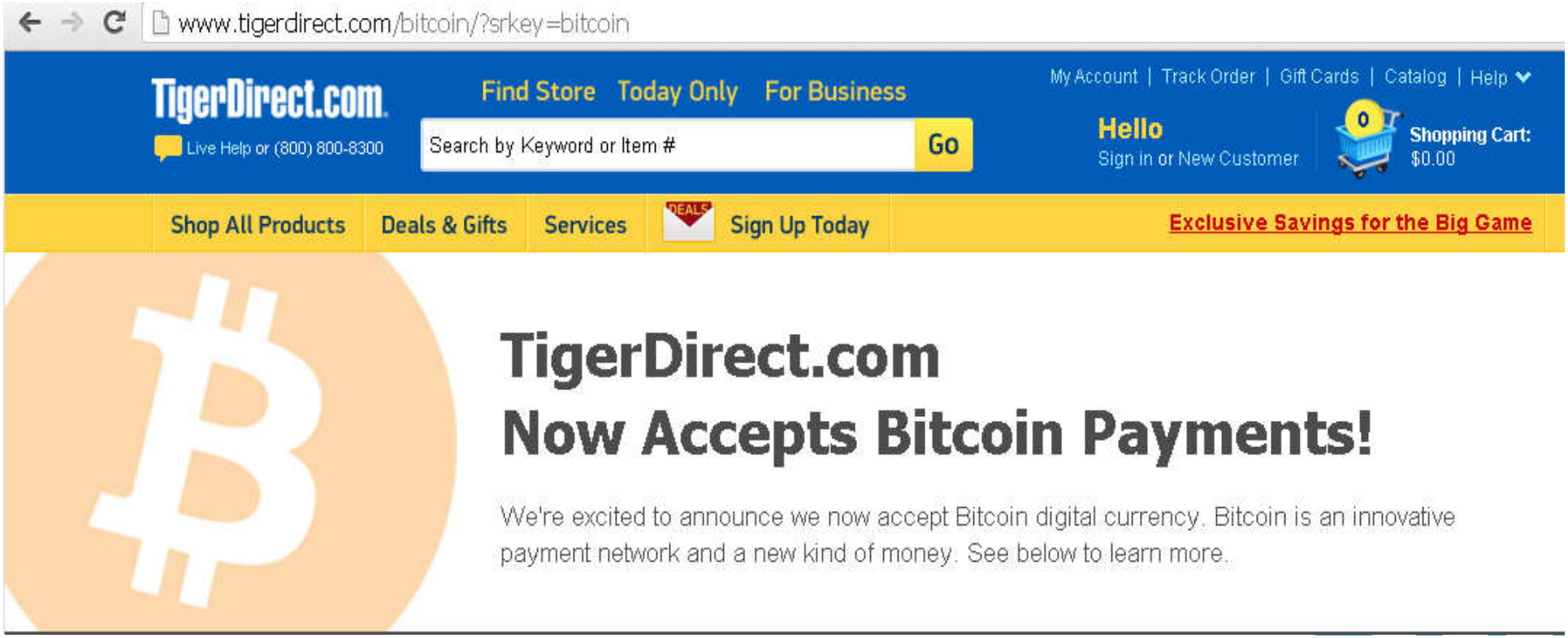
Geography – Peer Network

See bitnodes-project



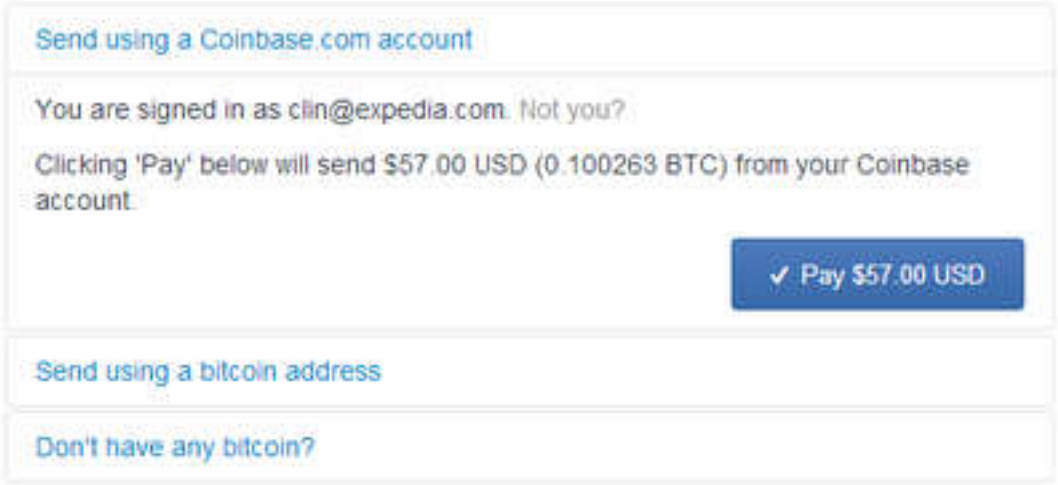
Bitcoin In Practice

Who Accepts Bitcoin? (1)



Who Accepts Bitcoin? (2)

Expedia



Overstock.com

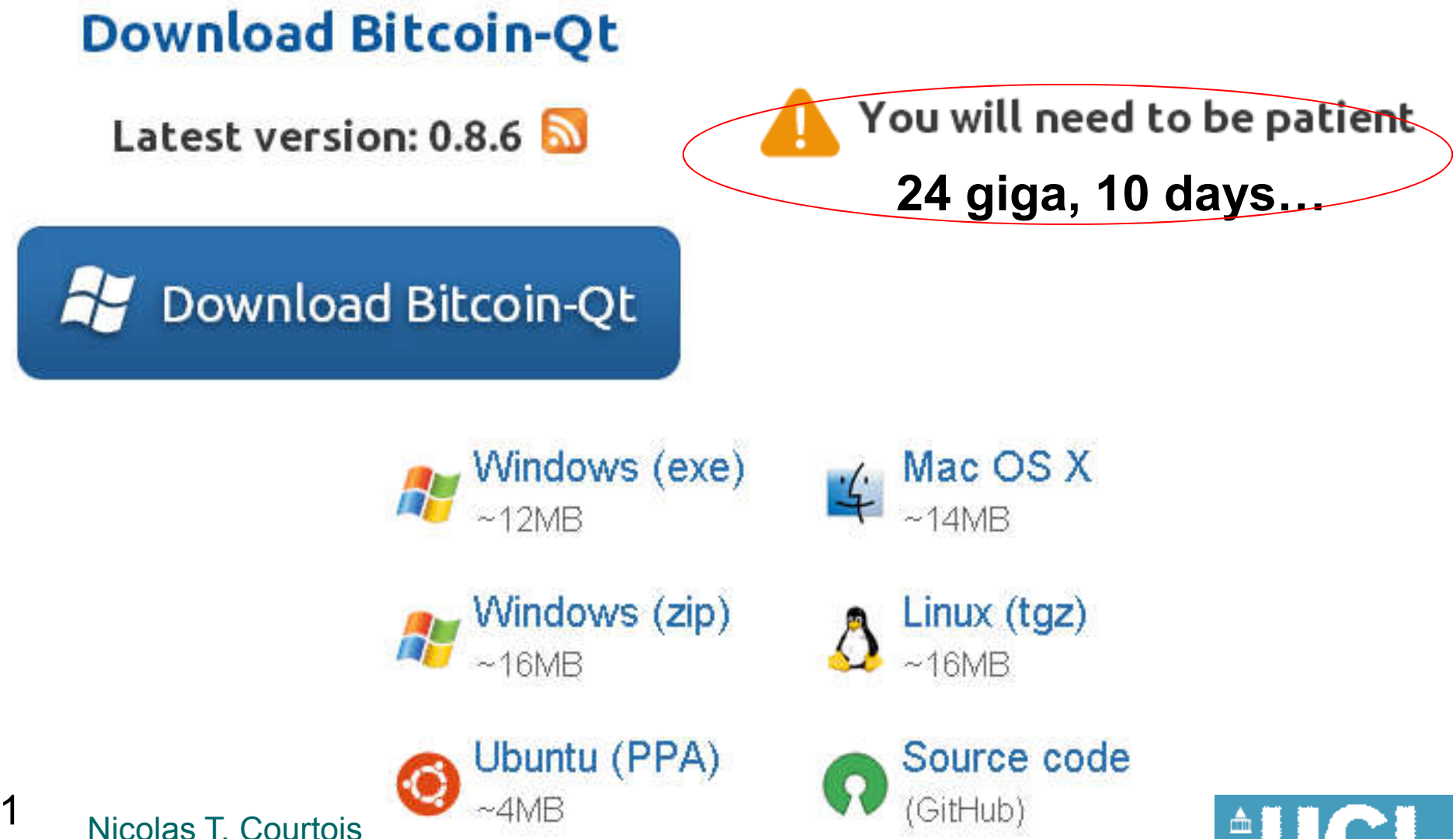
$20M in 2014?

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)

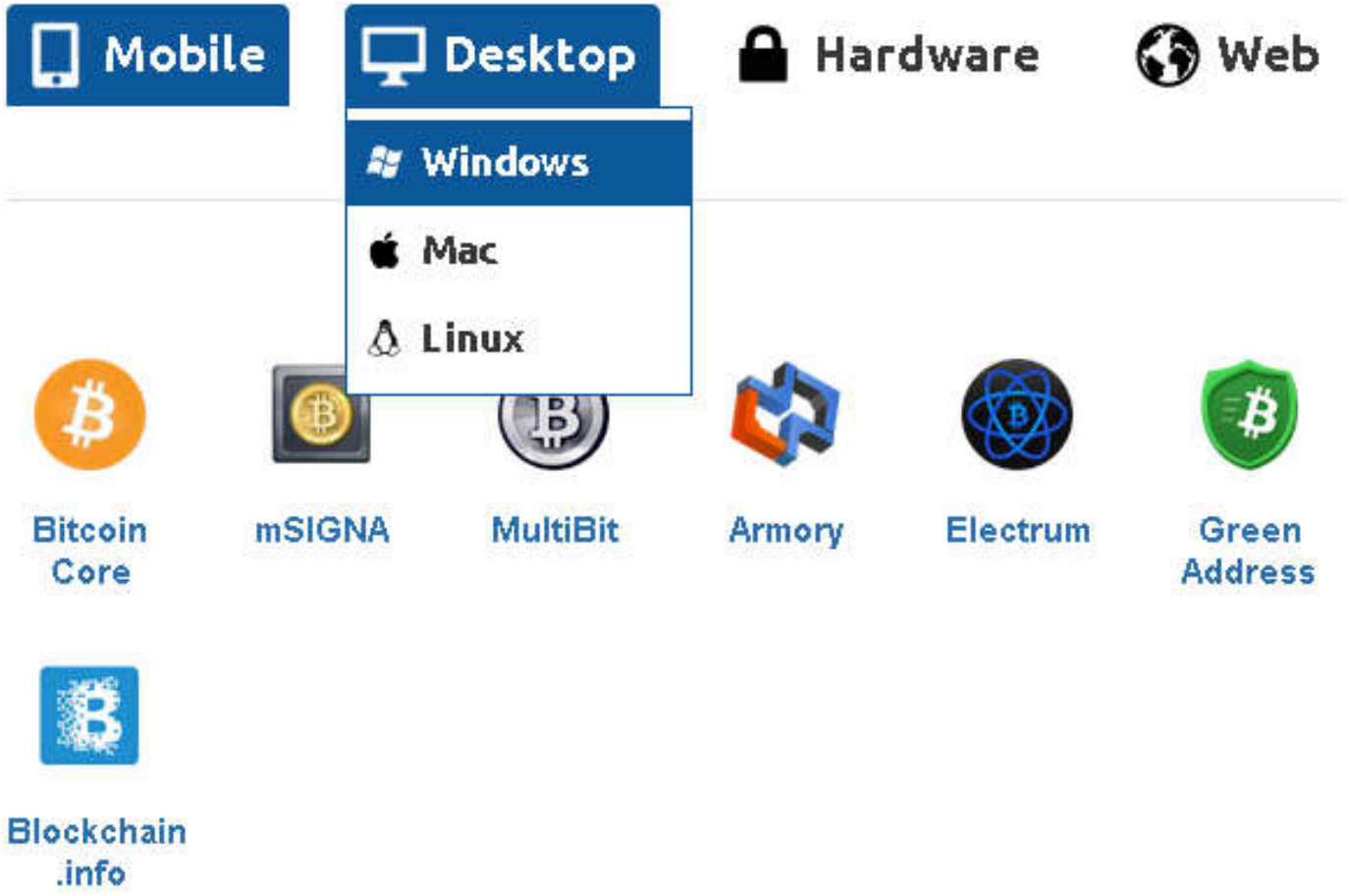
Full P2P Client

http://bitcoin.org/en/download

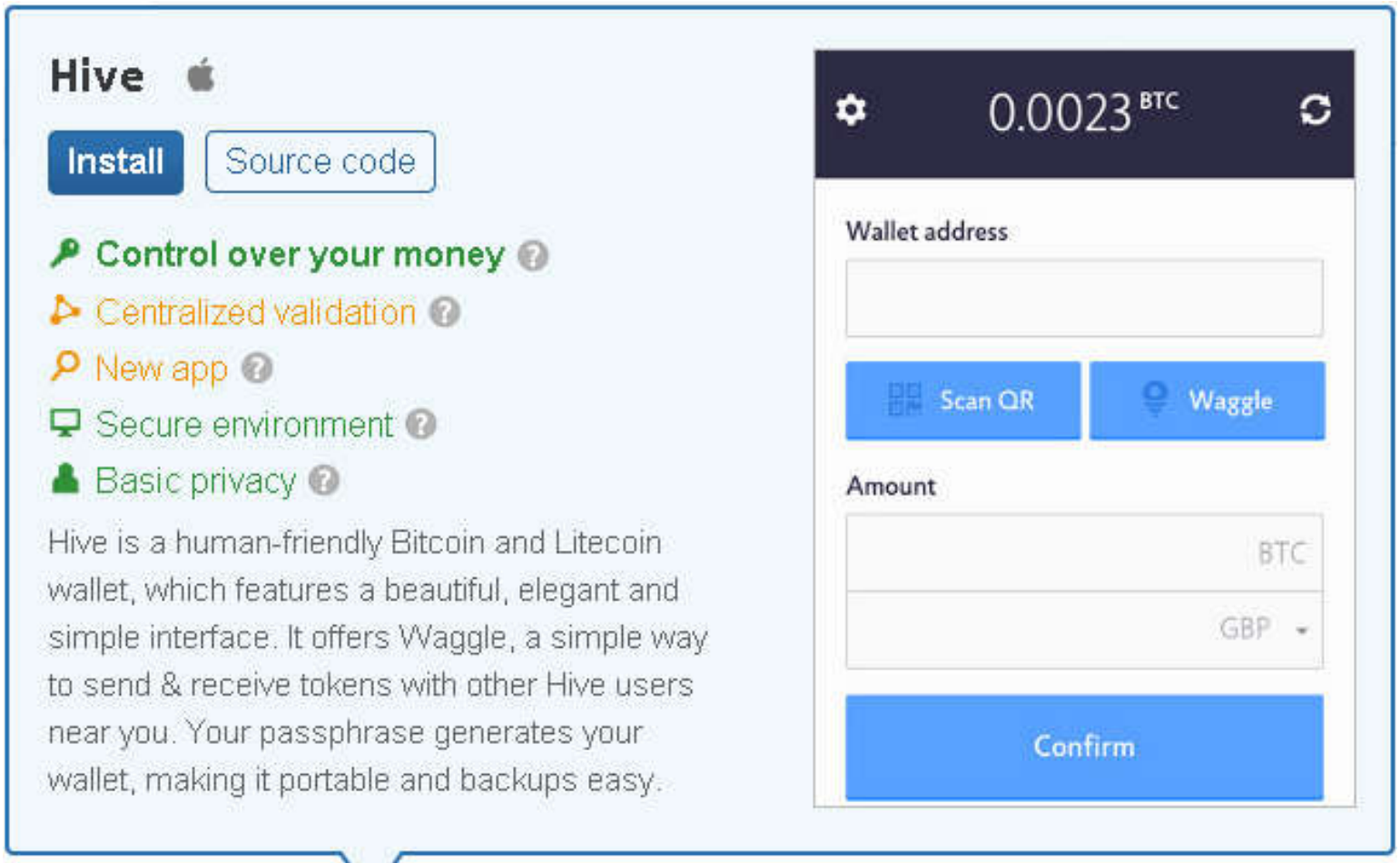


Comparison - PC

https://bitcoin.org/en/choose-your-wallet

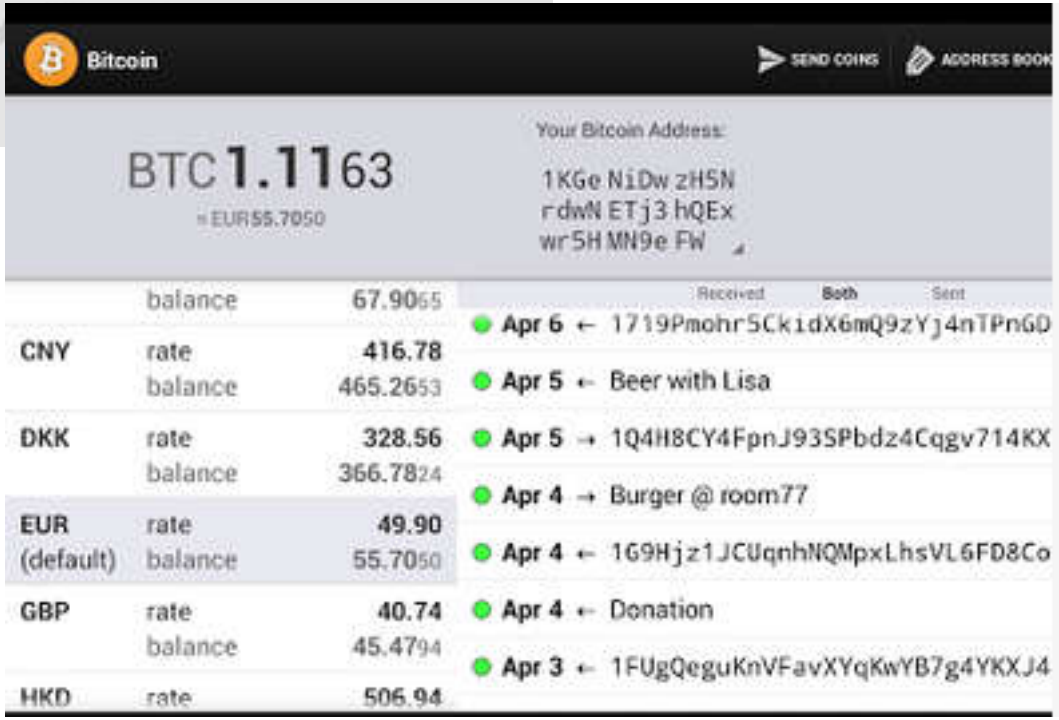


Mobile Phones



breadwallet Hive Blockchain .info Green Address

Mobile Apps - Android



Exchange Bitcoins <=> GBP

Why Coinfloor?

- City of London based, HMRC approved Bureau de Change
- The only exchange with 100% multi-signature cold storage
- Superior exchange performance, built for speed, scalability and security
- The first provably solvent bitcoin exchange

The Ascent Of Bitcoin

Crazy Ride


10-11 April 2013 – MtGox 24h shutdown
250
200
150
100
50
0
Market Price (USD)
The correction stops
Source: blockchain.info
13 April 2013 – "Digital Gold"
Nov '12
Dec '12
Jan '13
Feb '13
Mar '13
Apr '13
May '13
Jun '13
Jul '13
Aug '13
Sep '13
Oct '13

13 April 2013

The Economist

Virtual currencies

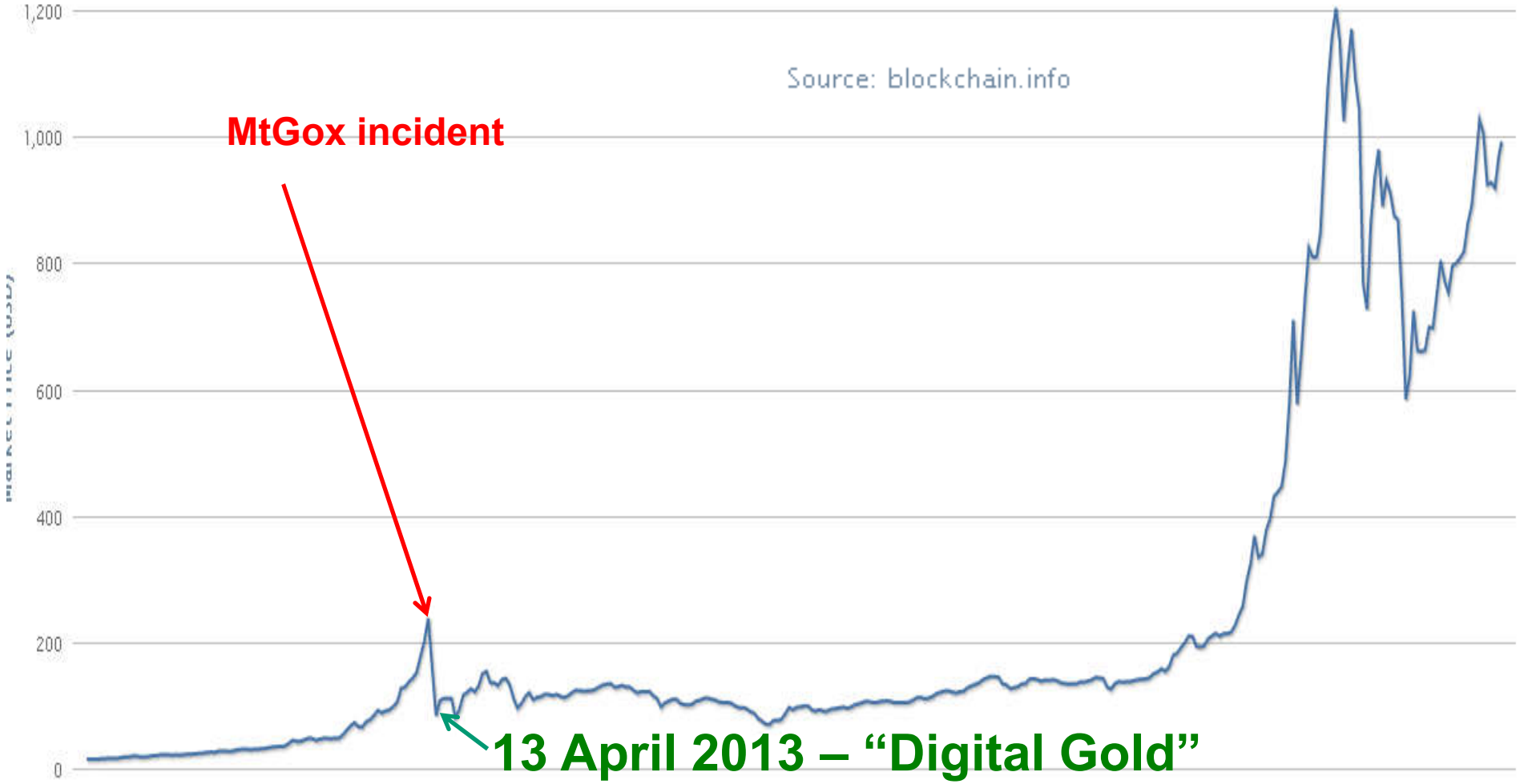
Mining digital gold

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

Apr 13th 2013 | From the print edition

Jan 2013-Jan 2014

14 => 1000 USD



2016: first doubled 400=>800 then back to 1000 USD levels

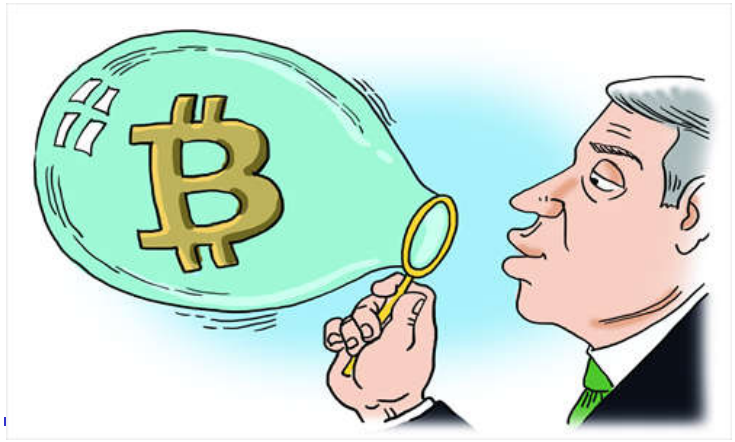
“Bots Caused Bitcoin Bubble”

Anonymously published Willy Report:

- algorithms, named Markus and Willy, bought up 650,000 bitcoins in the dying days of the MtGox exchange, causing the price of bitcoin to soar above $1,000.
- “there is a ton of evidence to suggest that all of these accounts were controlled by MtGox themselves“
- “so if you were wondering how bitcoin suddenly appreciated in value by a factor of 10 within the span of one month, well, this may be why."
- …also claimed to be bought with customer money

http://www.ibtimes.co.uk/cryptocurrency-news-round-mtgox-bots-caused-bitcoin-bubble-darkcoin-dives-1450415

Another Nobel Price:



In Davos Jan 2014:

"It is a bubble,
there is no question about it.
… It's just an amazing example of a bubble."

– Robert Shiller, Nobel price in economics, awarded specifically for work on asset bubbles.

Bitcoin Mining

Money Out of Thin Air

Bitcoin vs. Klondike

2012-2014

>100,000 miners

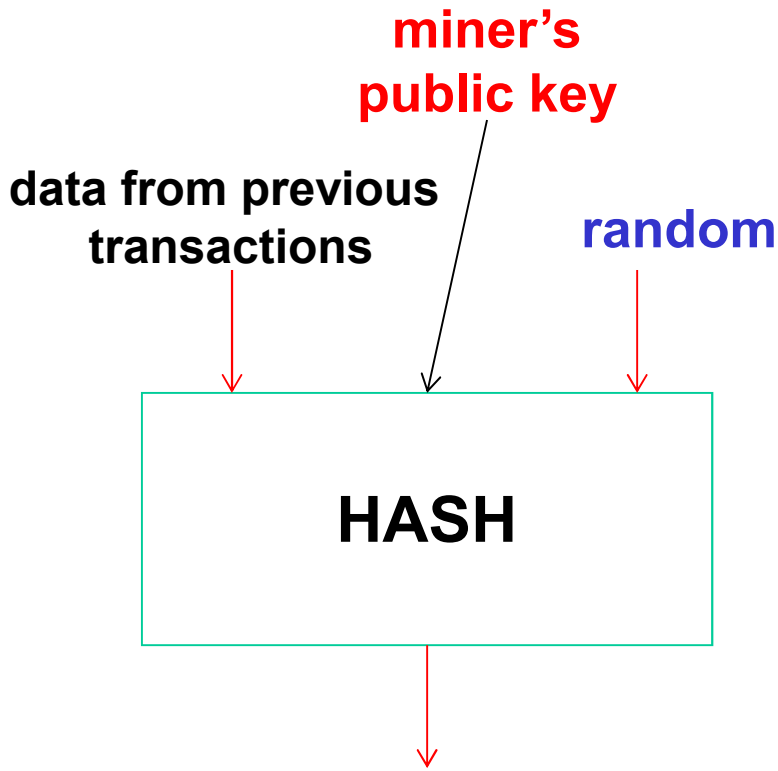
maybe ½ - ¾???? were victims of scams and paid for miners which were not delivered in reasonable time

1896-1899
100,000 miners,
4,000 struck gold

Bitcoin Mining

- Minting: creation of new currency.

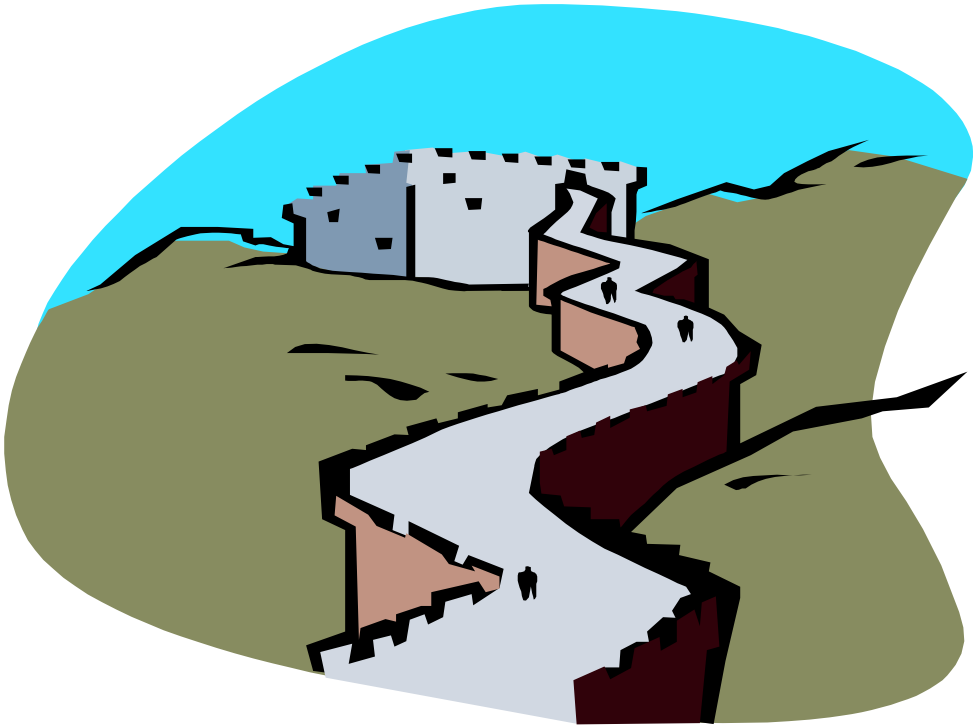
Creation of "money"
+re-confirmation
of older transactions



Hash Power => Security???

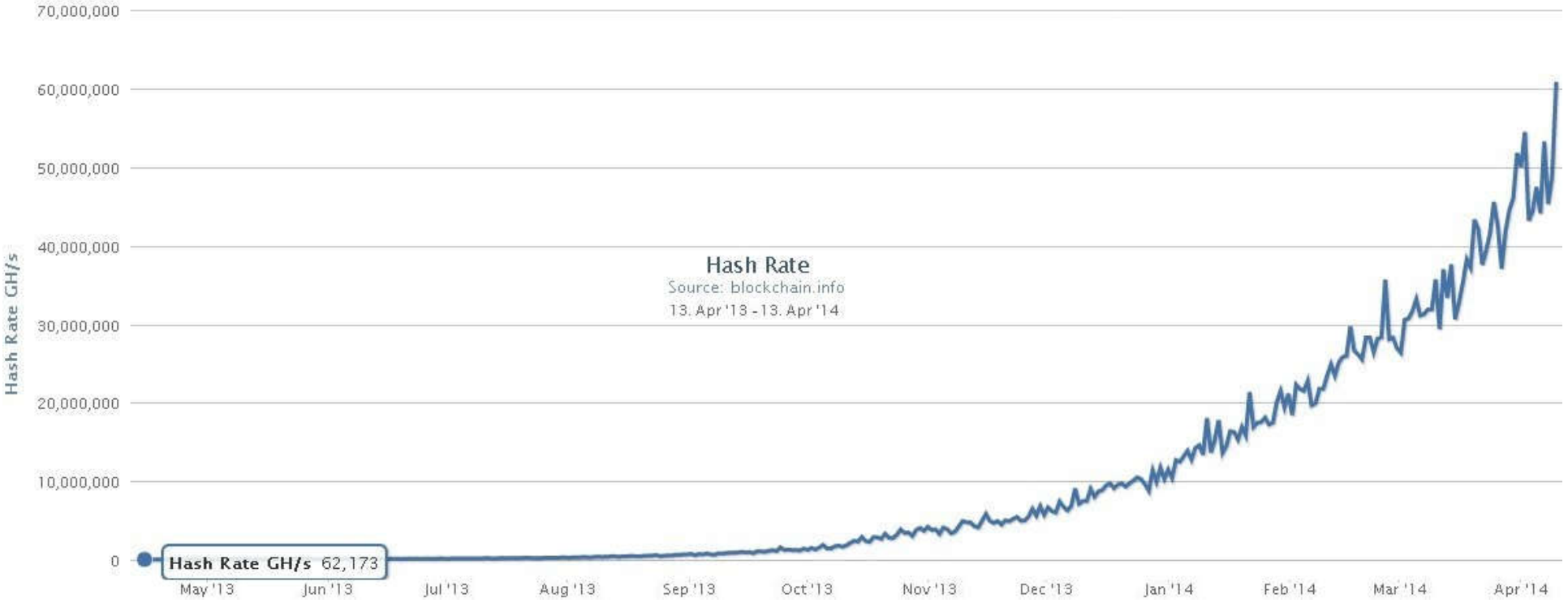
Sams writes: "The amount of capital collectively burned hashing fixes the capital outlay required of an attacker […] to have a meaningful chance of orchestrating a successful double-spend attack […]

REMARK:
THIS IS MISTAKEN,
read my papers



Crazy Hash Power Increase

Nearly doubled every month… 1000x in 1 year.

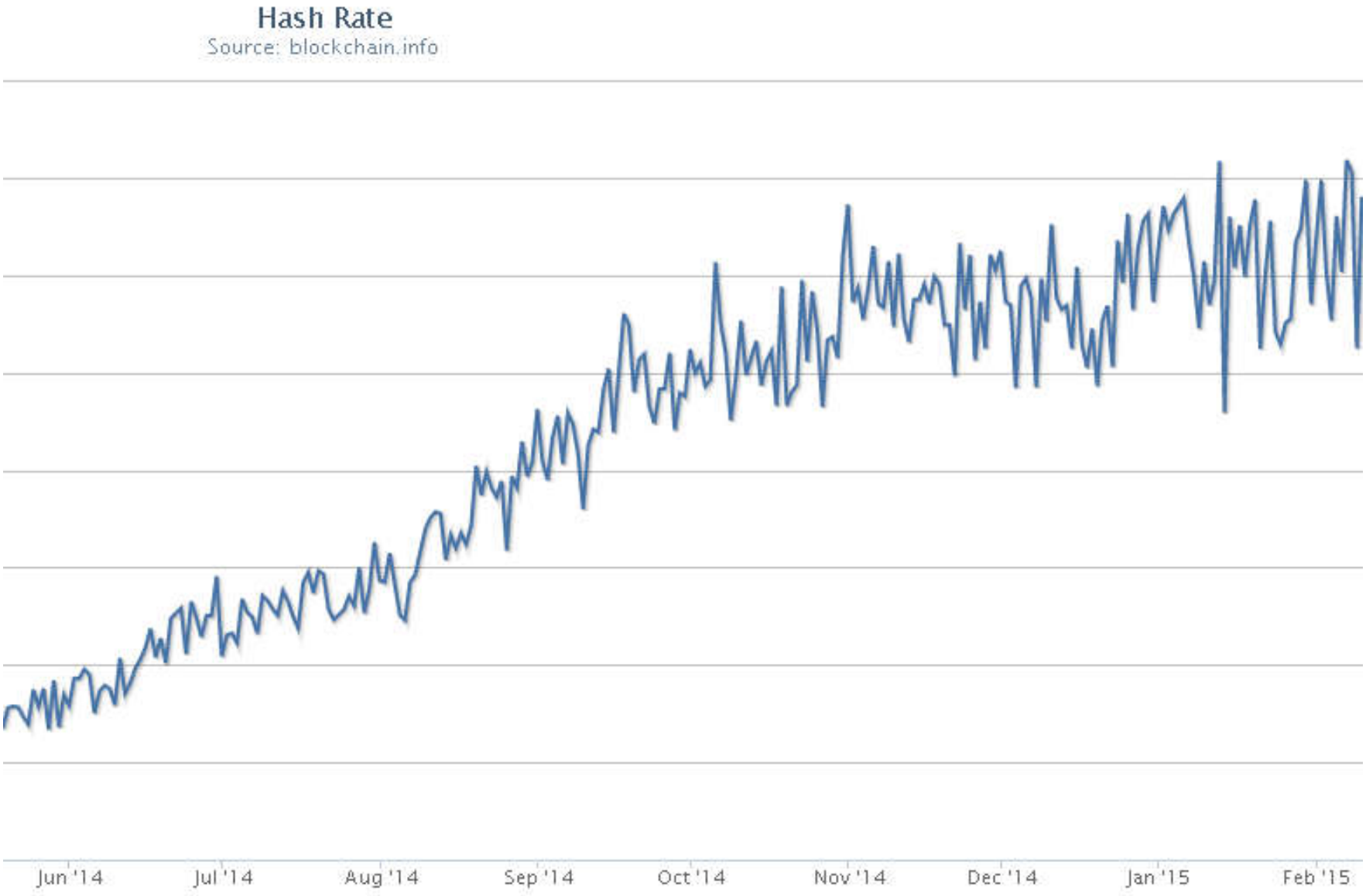


Thm:

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

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

Jan 2015: Peak Reached



Bitcoin!

A payment system in which

- it is THE PAYER who initiates the transaction
- controls the amount being paid
- money and payments are stored outside of the banking system [most recent systems erode the dominant position of banks]
- money cannot be confiscated [cf. Cyprus banks].
- it challenges fractional reserve banking [new!] and forces finance to become more “transparent”

“Troubled” bitcoin [The Economist May 2014] is here to stay

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

UCL Bitcoin Seminar

blog.bettercrypto.com / SEMINAR