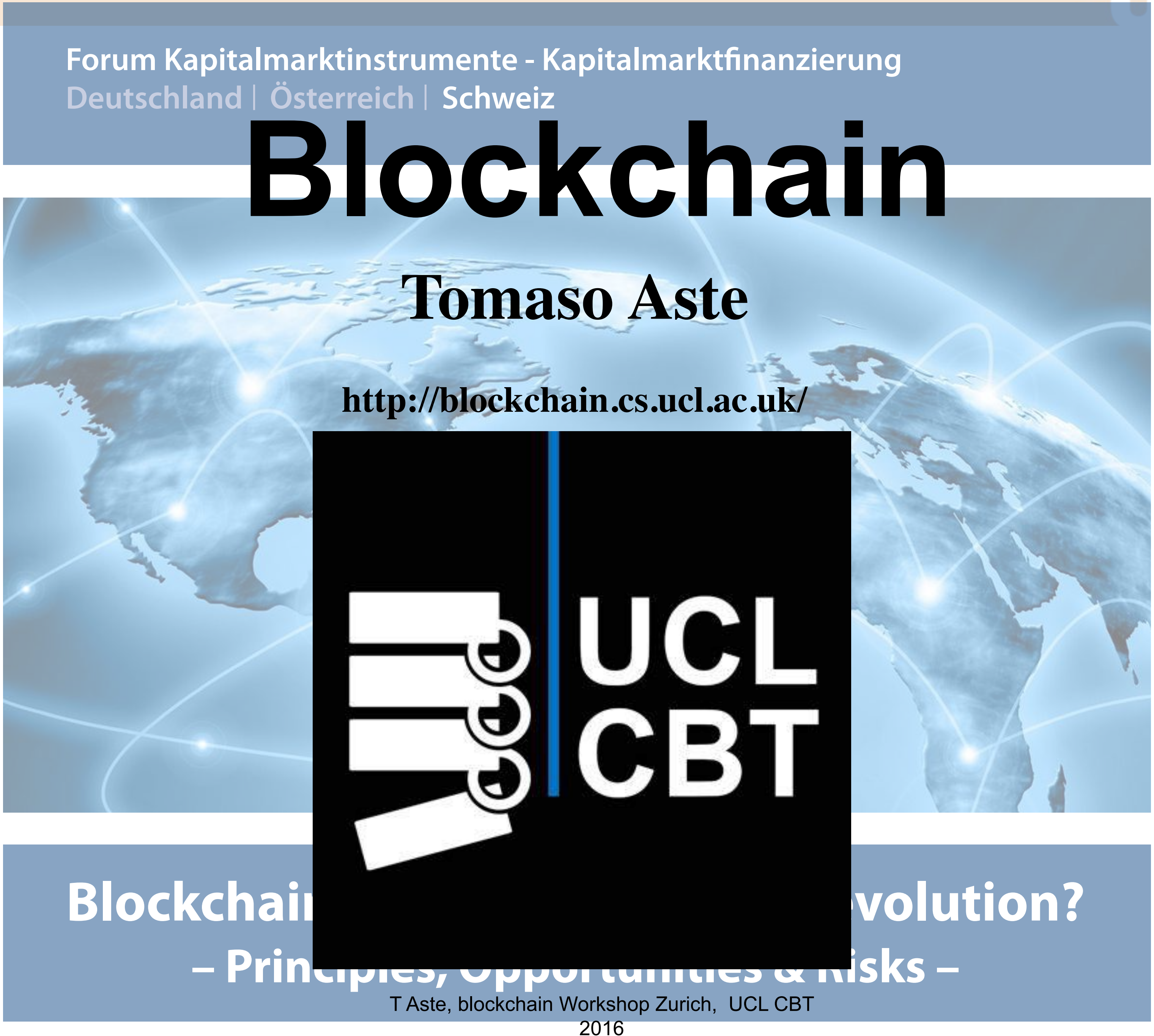


Forum Kapitalmarktinstrumente - Kapitalmarktfinanzierung
Deutschland | Österreich | Schweiz

Blockchain

Tomaso Aste

http://blockchain.cs.ucl.ac.uk/

Blockchai ... volution?

– Prin ... isks –

Forum Kapitalmarktinstrumente - Kapitalmarktfinanzierung

Deutschland | Österreich | Schweiz

Program

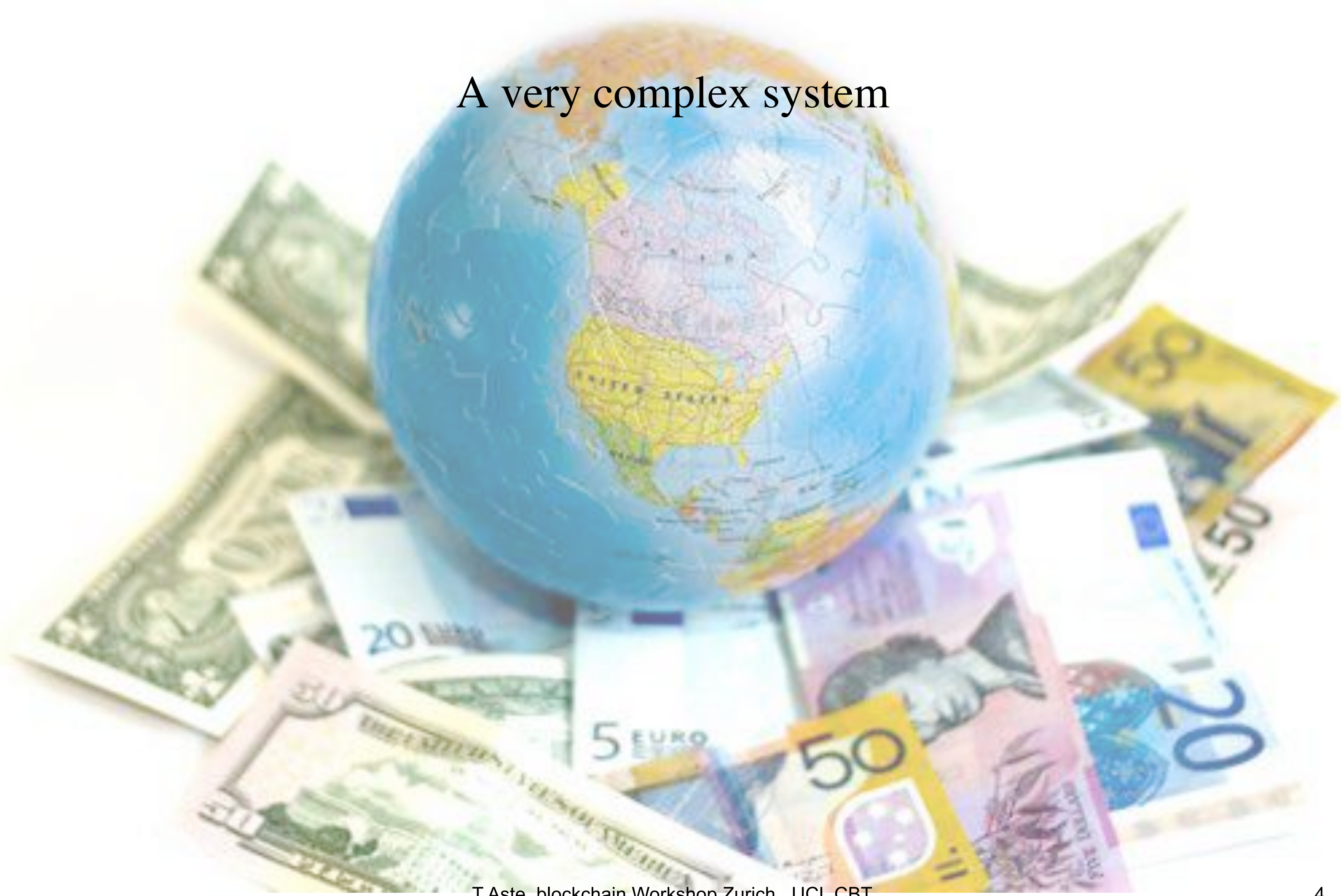
09.30 - 10.00	Registration
10.00 - 10.15	Welcoming & Introduction by Raoul Würgler
10.15 - 11.15	**Module 1: General introduction and important concepts by Prof. Dr. Tomaso Aste** - What is money? Why is Bitcoin money? - The disruptive character of Bitcoin - Bitcoin: a 10-minute primer - Live payment demo - Introduction to the crypto in crypto-currencies - Bitcoin: a truly decentralized architecture
11.15 - 12.15	**Module 2: Mining: basic principles, consequences, and associated ecosystem by Prof. Dr. Tomaso Aste** - Hash functions, mining difficulty - Mining tools - Is mining beneficial? Gold rush syndrome - Mining pools, mining farms, cloud mining

What is money?

A trusted medium of exchange that makes trading efficient

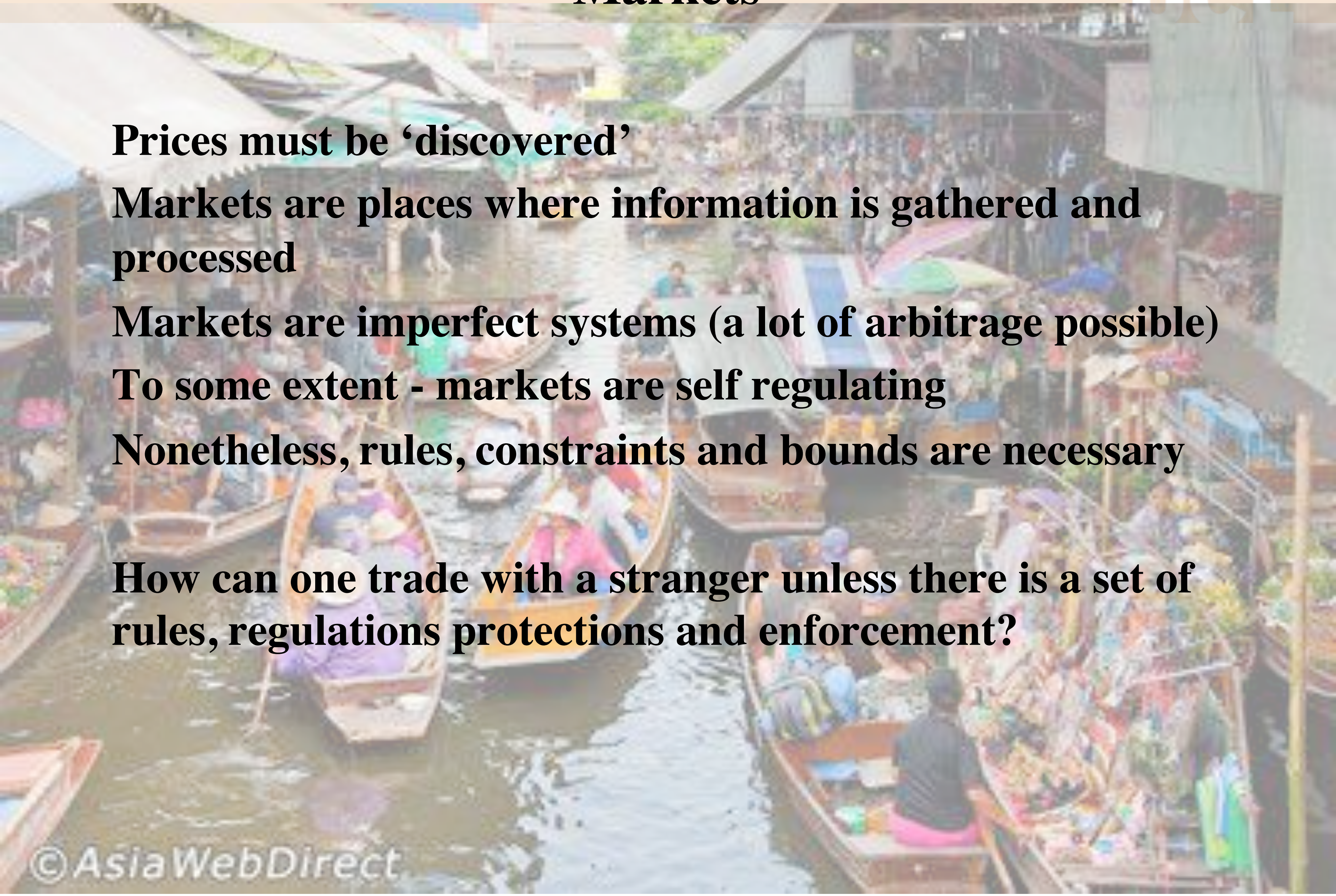
Economy

A very complex system



Digital Economy

Markets



Prices must be ‘discovered’

Markets are places where information is gathered and processed

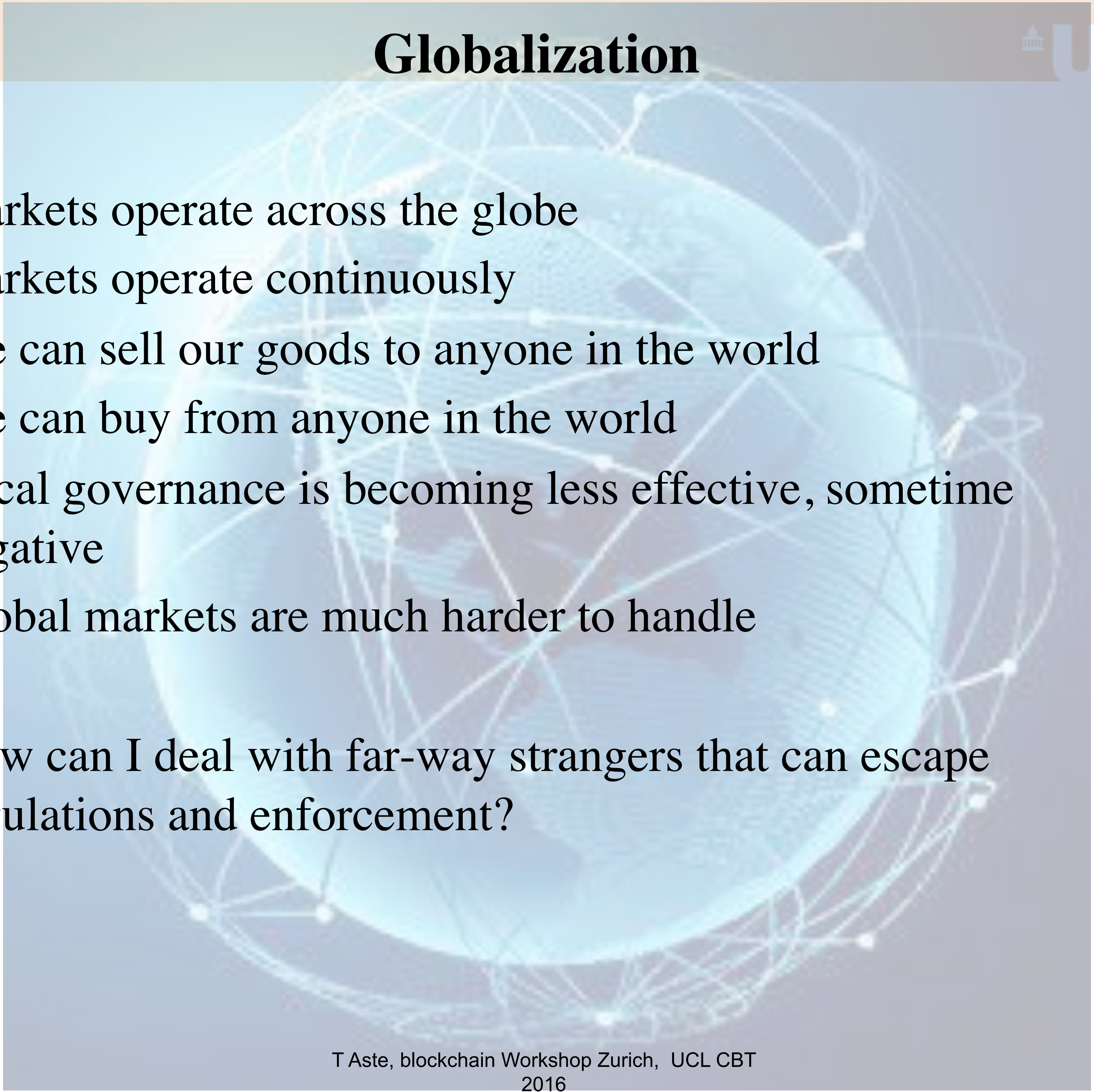
Markets are imperfect systems (a lot of arbitrage possible)

To some extent - markets are self regulating

Nonetheless, rules, constraints and bounds are necessary

How can one trade with a stranger unless there is a set of rules, regulations protections and enforcement?

Globalization



Markets operate across the globe

Markets operate continuously

We can sell our goods to anyone in the world

We can buy from anyone in the world

Local governance is becoming less effective, sometime negative

Global markets are much harder to handle

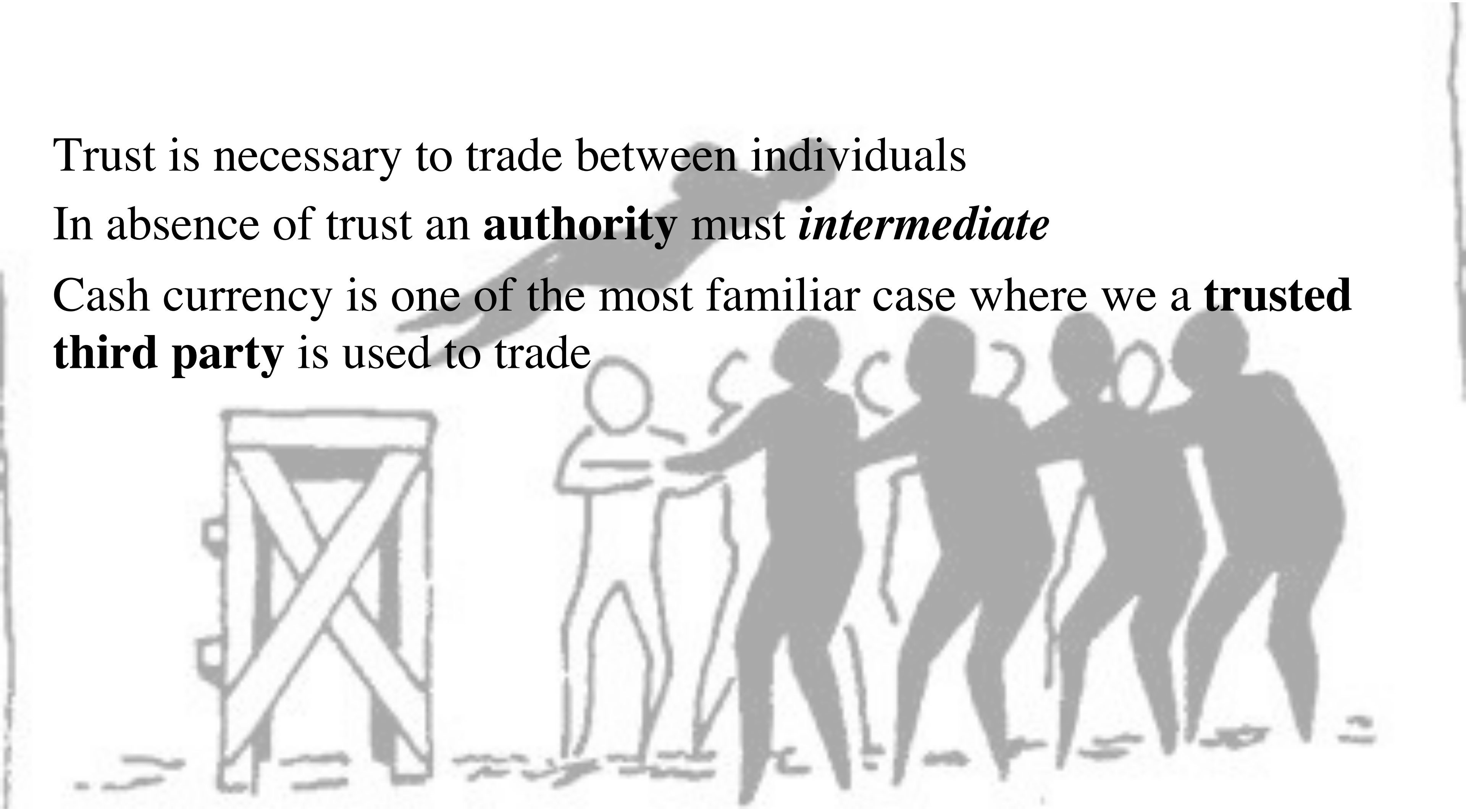
How can I deal with far-way strangers that can escape regulations and enforcement?

Trust

Trust is necessary to trade between individuals

In absence of trust an **authority** must ***intermediate***

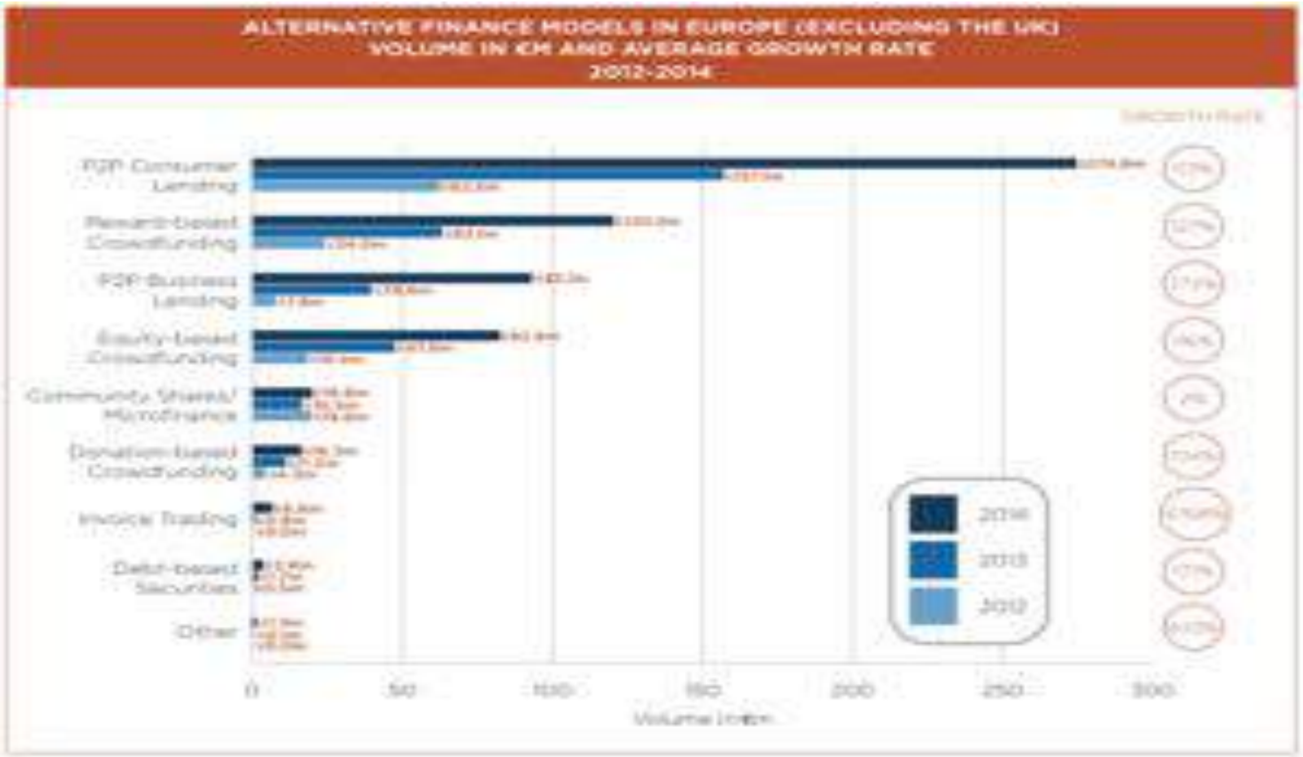
Cash currency is one of the most familiar case where we a **trusted third party** is used to trade



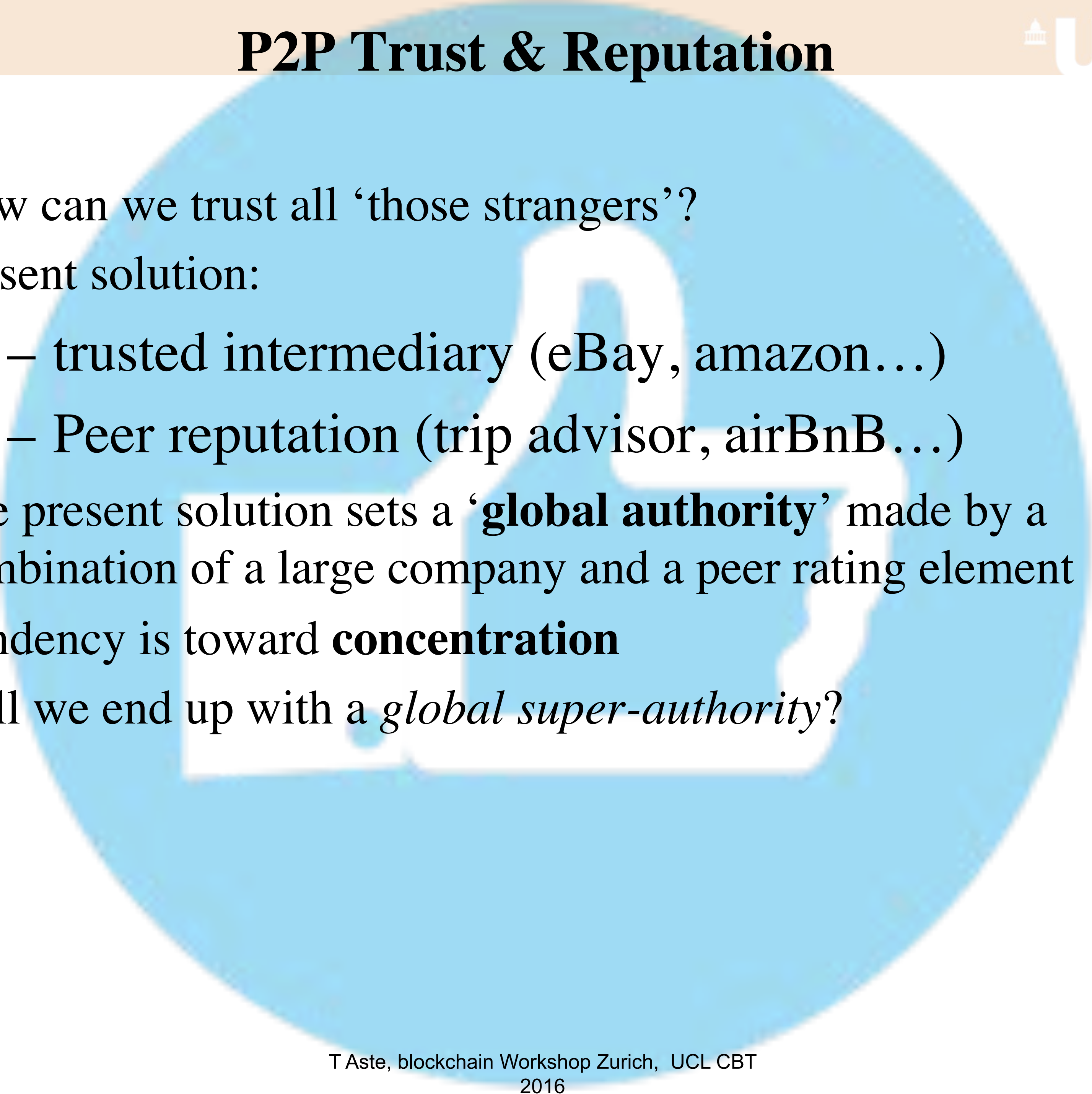
Digital Economy

Technology can put in contact individuals form far away parts of the world

Peer – to – peer economy is growing fast within The Internet



P2P Trust & Reputation



How can we trust all ‘those strangers’?

Present solution:

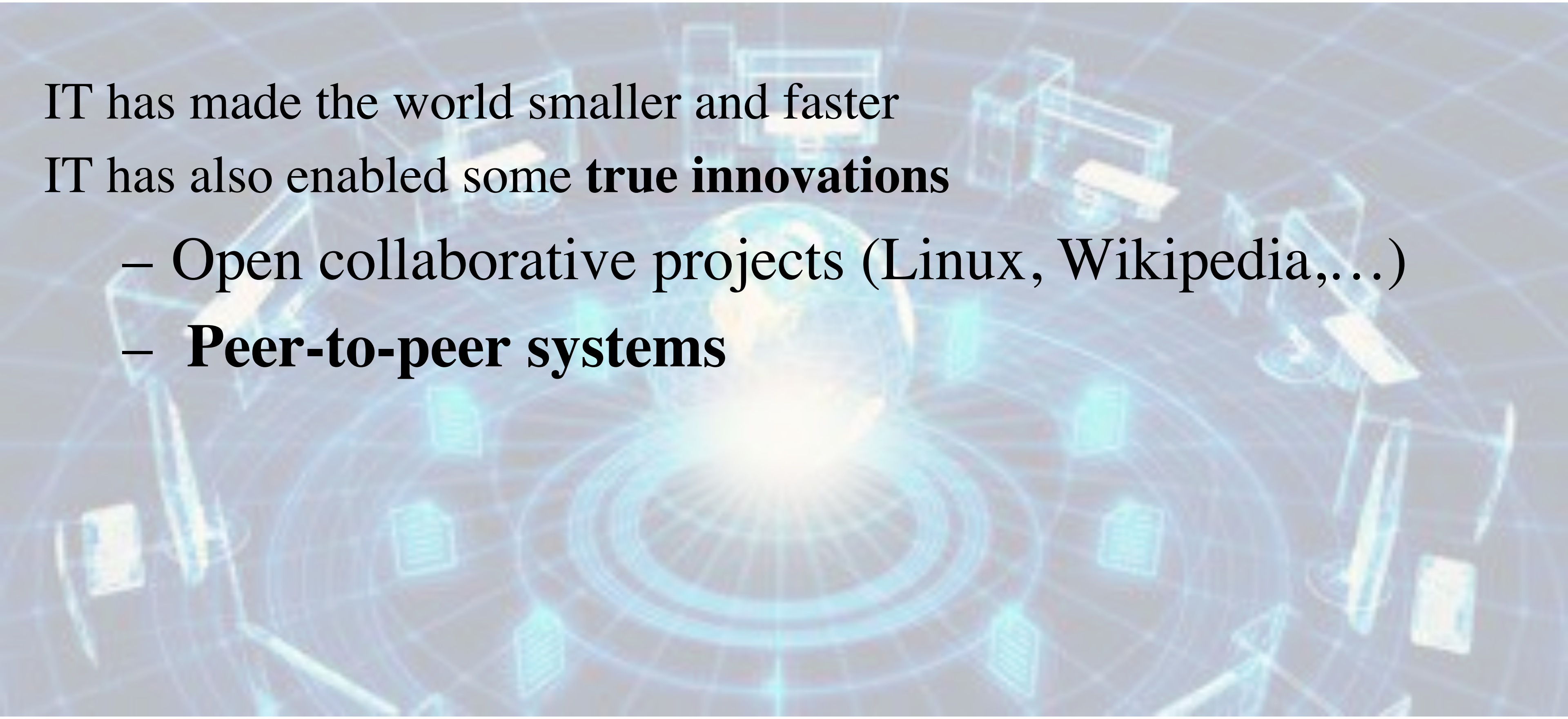
- trusted intermediary (eBay, amazon…)
- Peer reputation (trip advisor, airBnB…)

The present solution sets a ‘**global authority**’ made by a combination of a large company and a peer rating element

Tendency is toward **concentration**

Will we end up with a *global super-authority*?

Information Technology

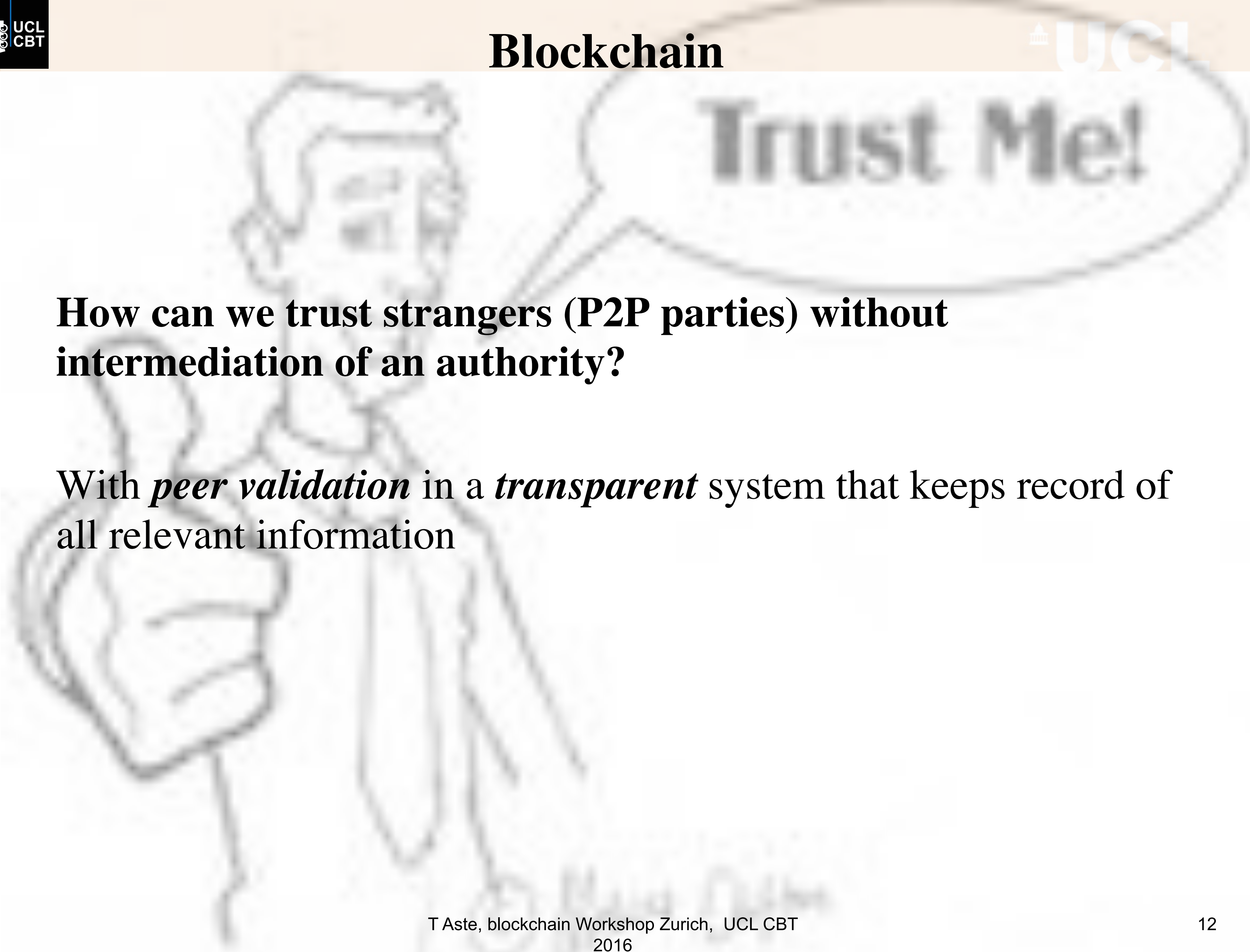


IT has made the world smaller and faster

IT has also enabled some **true innovations**

- – Open collaborative projects (Linux, Wikipedia,…)
- – **Peer-to-peer systems**

Blockchain

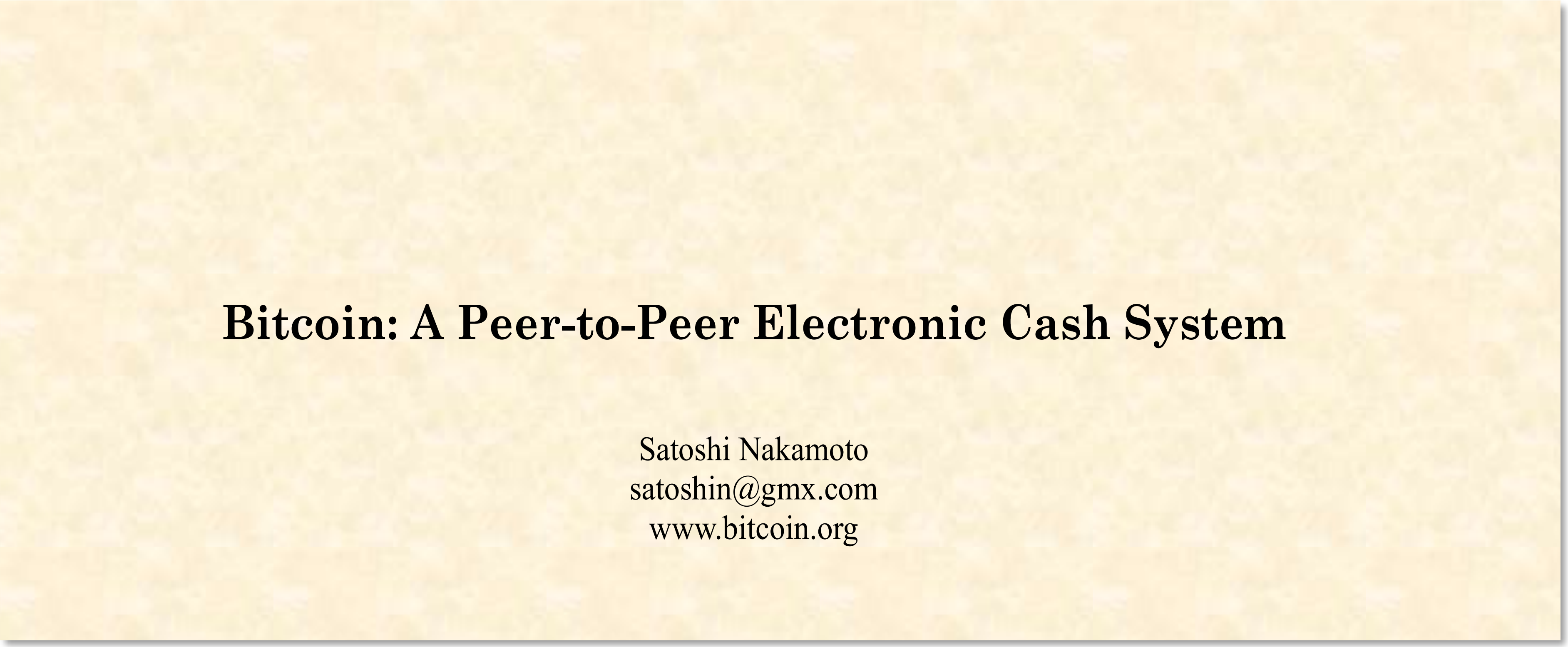


How can we trust strangers (P2P parties) without intermediation of an authority?

With ***peer validation*** in a ***transparent*** system that keeps record of all relevant information

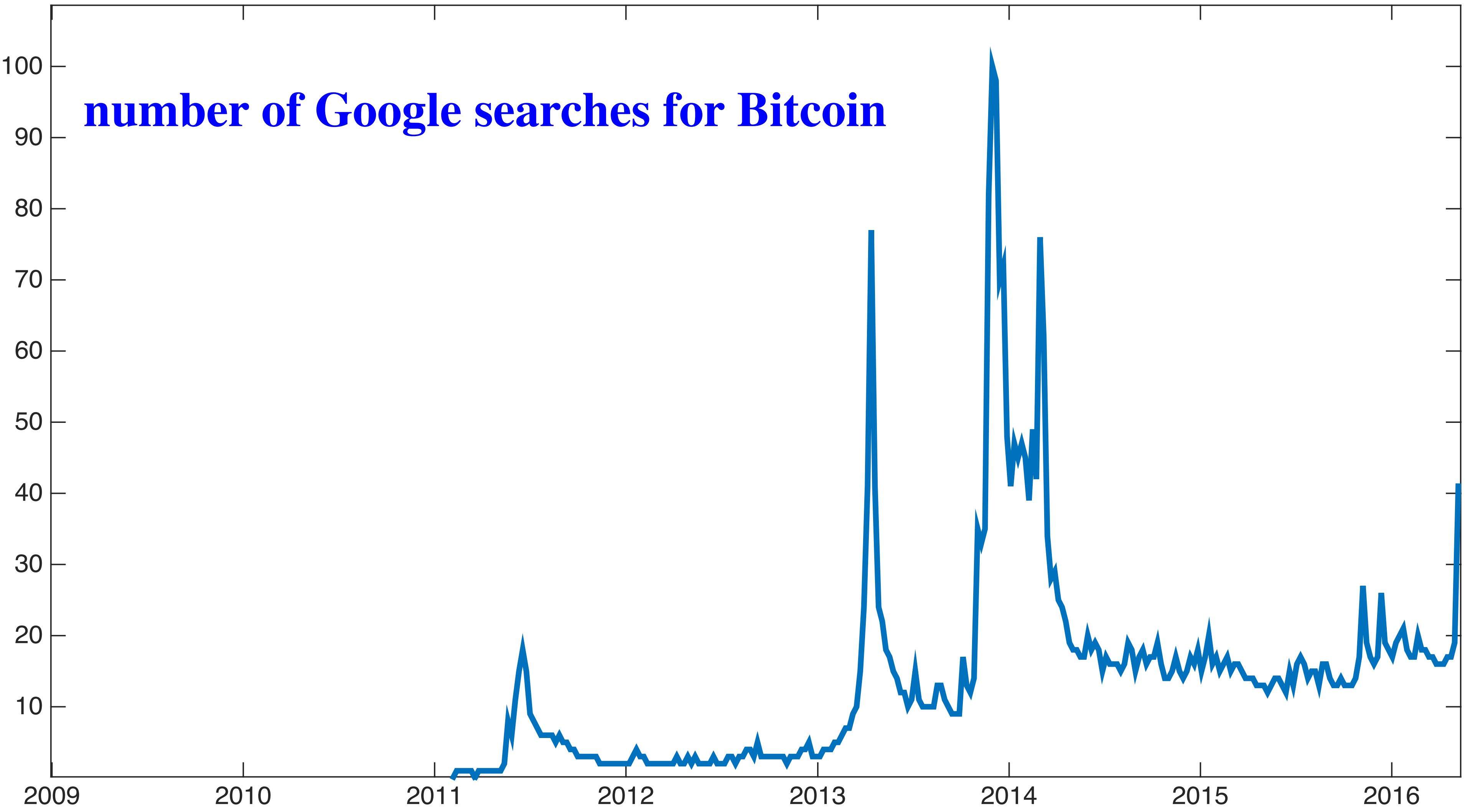
The disruptive character of Bitcoin

2008

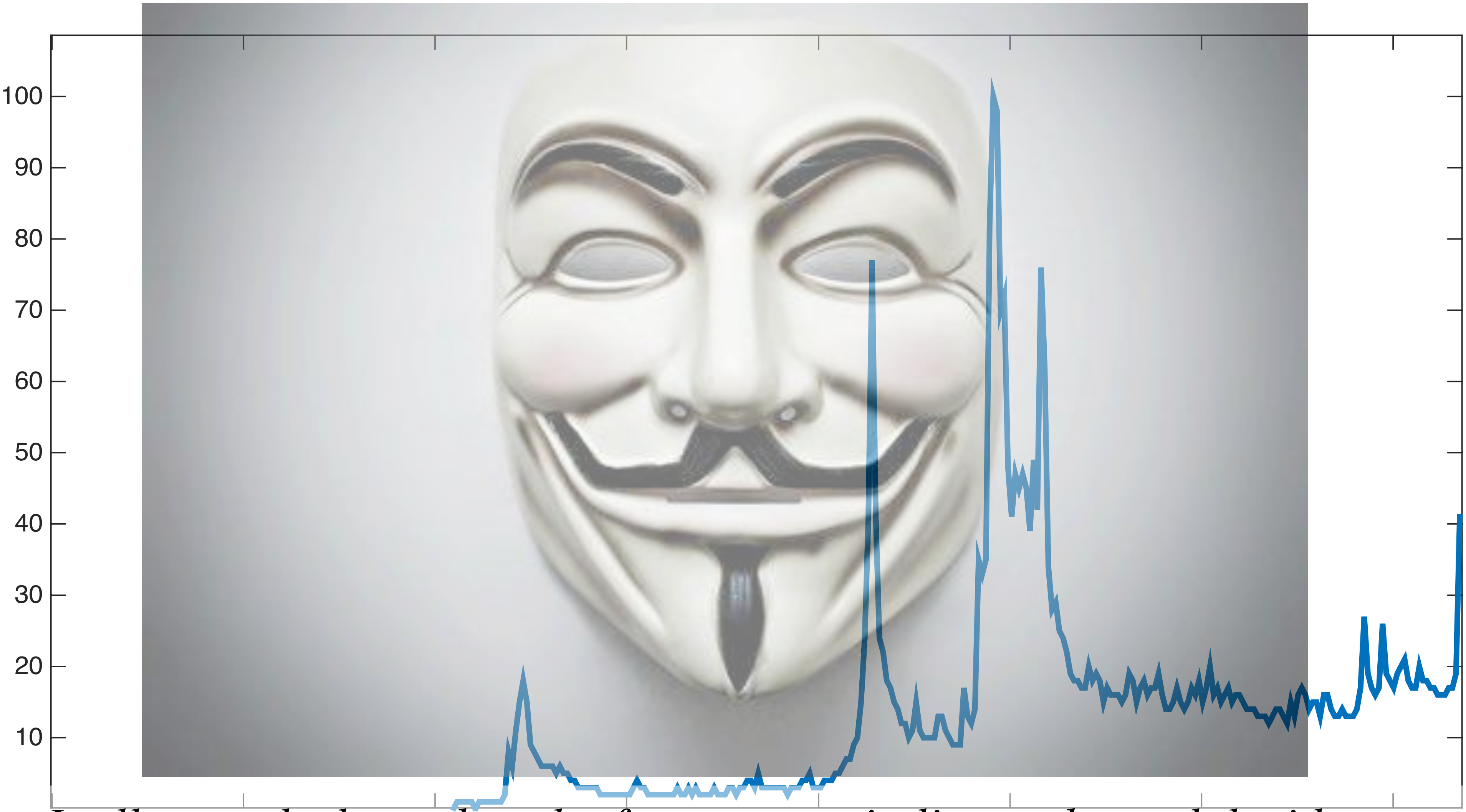


Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org


number of Google searches for Bitcoin
100
90
80
70
60
50
40
30
20
10
2009
2010
2011
2012
2013
2014
2015
2016

Blockchain



It all started when a bunch of anarco-capitalists embraced the idea to have a currency not issued by a state

Bitcoin

- Pure **peer-to-peer digital cash** that does not need third party authority and anyone can use it
- Introduced in 2009 by Satoshi Nakamoto it has presently 6 billion dollar capitalization
- All transactions are kept in a shared, single but replicated and distributed bookkeeping source (**ledger**)
- Every participant (**node**) has a ledger replica
- Nodes synchronize the ledger periodically by verifying and approving **blocks** of transactions
- Coins are protected by cryptographic keys and only the owner of the private key can spend the coin
- The validity of a block is established by the next block attaching to it with a cryptographic sealing
- The **block chain** is the chronological list of all blocks of transactions from the genesis block

Bitcoin: a decentralized architecture

Blockchain is a Distributed Ledger

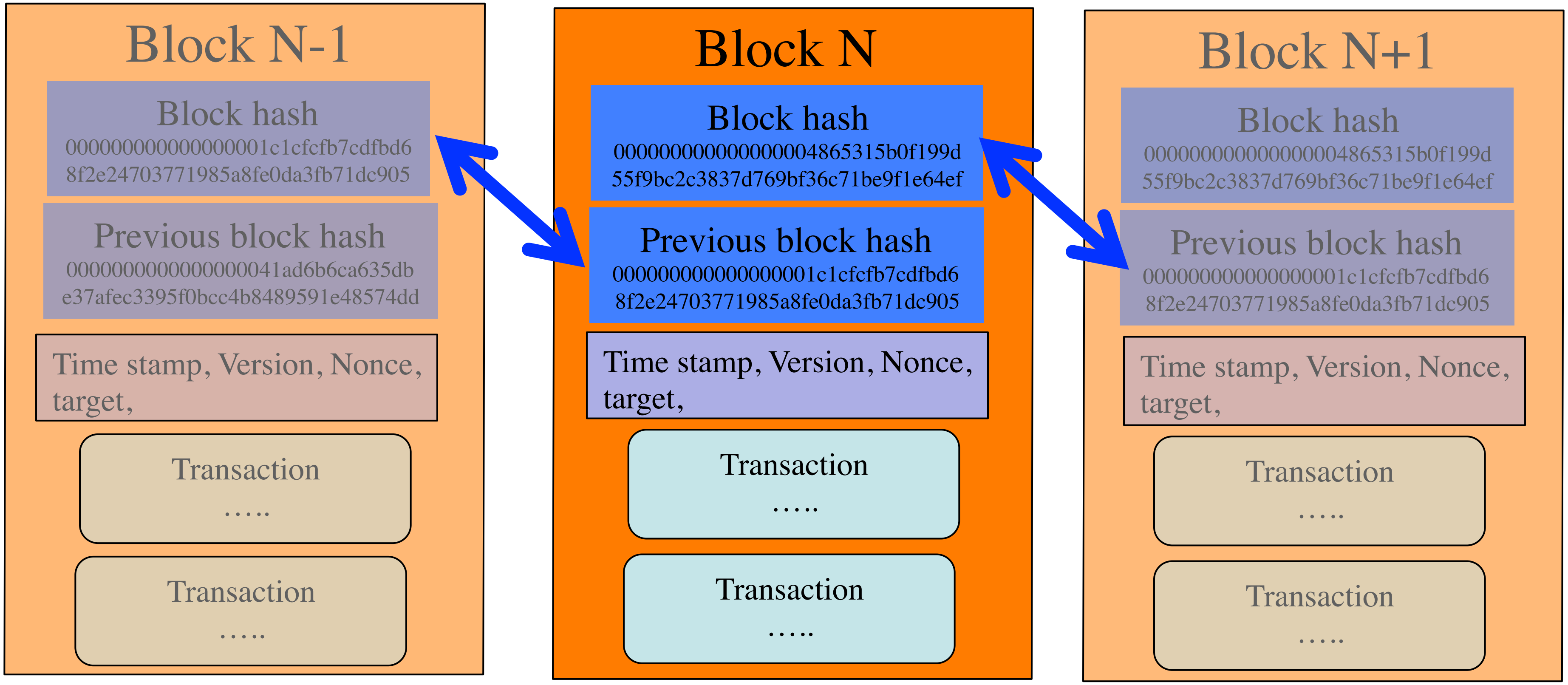
Every node in the network has a copy of the blockchain which records all transactions up to the point when the first coin was mined

Transactions are publically announced on the networks and anyone can verify the authenticity of the data

To avoid double spending, the earliest transaction is the one that counts

Participants must agree on the order of the transactions

Blockchain



Block N-1

Block hash
000000000000000001c1cfcfb7cdfbd6
8f2e24703771985a8fe0da3fb71dc905

Previous block hash
00000000000000000041ad6b6ca635db
e37afec3395f0bcc4b8489591e48574dd

Time stamp, Version, Nonce, target,

Transaction
…..

Transaction
…..

Block N

Block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

Previous block hash
000000000000000001c1cfcfb7cdfbd6
8f2e24703771985a8fe0da3fb71dc905

Time stamp, Version, Nonce, target,

Transaction
…..

Transaction
…..

Block N+1

Block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

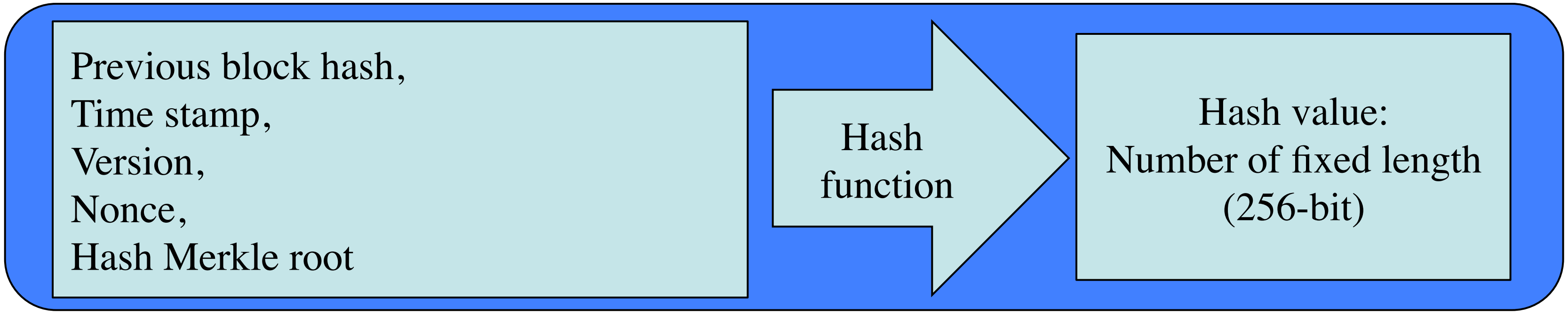
Previous block hash
000000000000000001c1cfcfb7cdfbd6
8f2e24703771985a8fe0da3fb71dc905

Time stamp, Version, Nonce, target,

Transaction
…..

Transaction
…..

Hashing



Previous block hash,
Time stamp,
Version,
Nonce,
Hash Merkle root

Hash function

Hash value:
Number of fixed length
(256-bit)

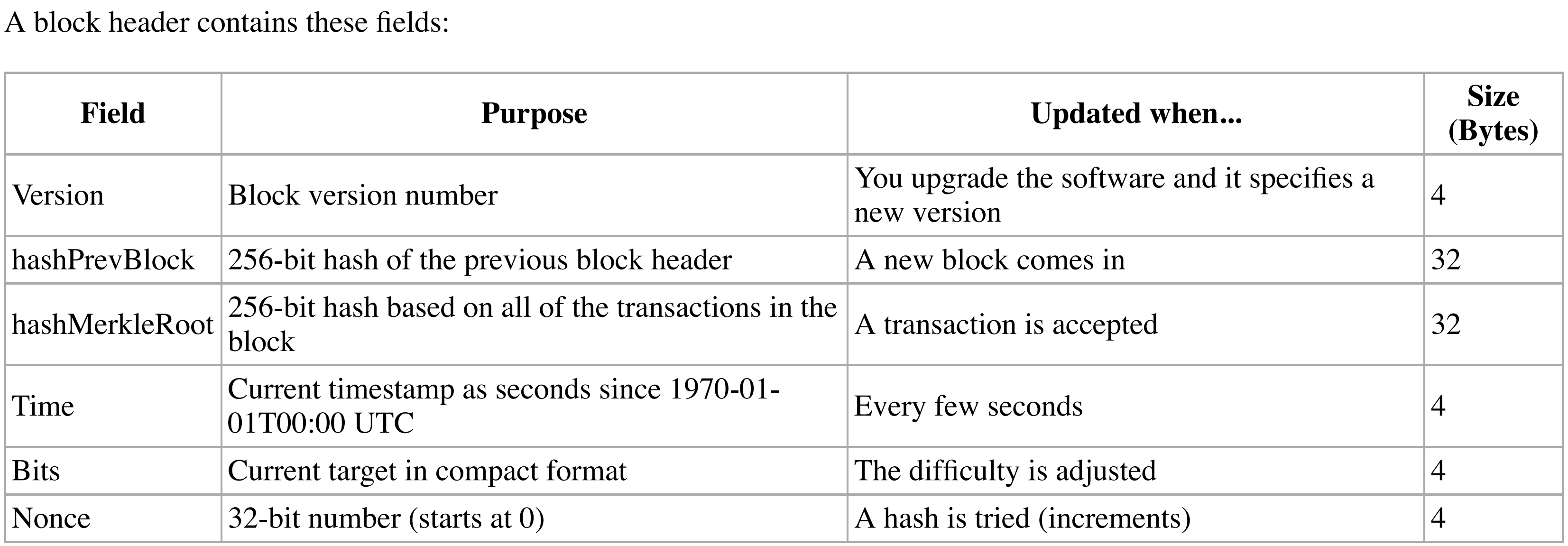
Some basic concepts
in
crypto-currencies

Unique hash

Hashing is a function that associate any digital input of any size to an output of fixed size

The output is easy to compute and the function is (practically) impossible to inverse

In bitcoin the input is the header of the block and the output is a 256bit number



A block header contains these fields:

Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	You upgrade the software and it specifies a new version	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4

https://en.bitcoin.it/wiki/Block_hashing_algorithm

Bitcoins are cryptographically protected

To receive a bitcoin one needs an **address**, the address is public

To spend a bitcoin one needs a **private key** that authorizes the transaction

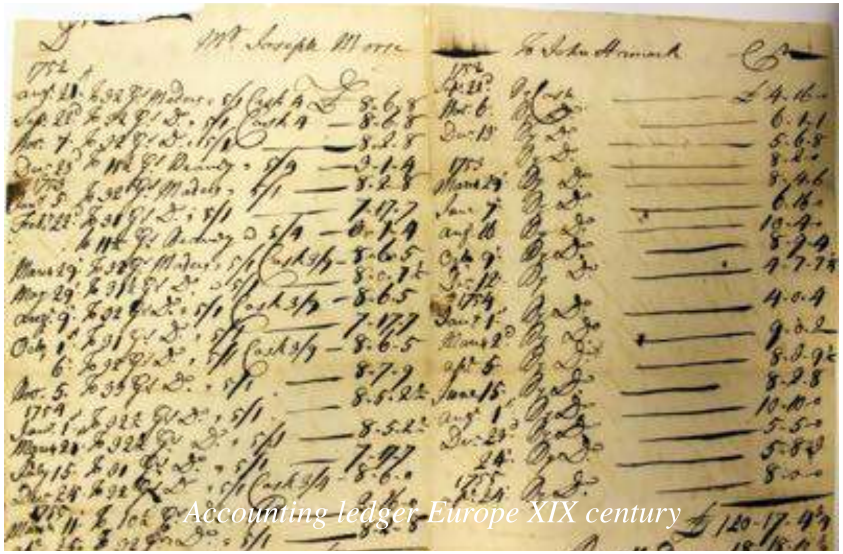
Address is created by picking a random number and creating a **public/private key couple** using the Elliptic Curve Digital Signature Algorithm

The address is a modified version of the public key

The disruptive character of Bitcoin?

What is the technological innovation?

The ledger?

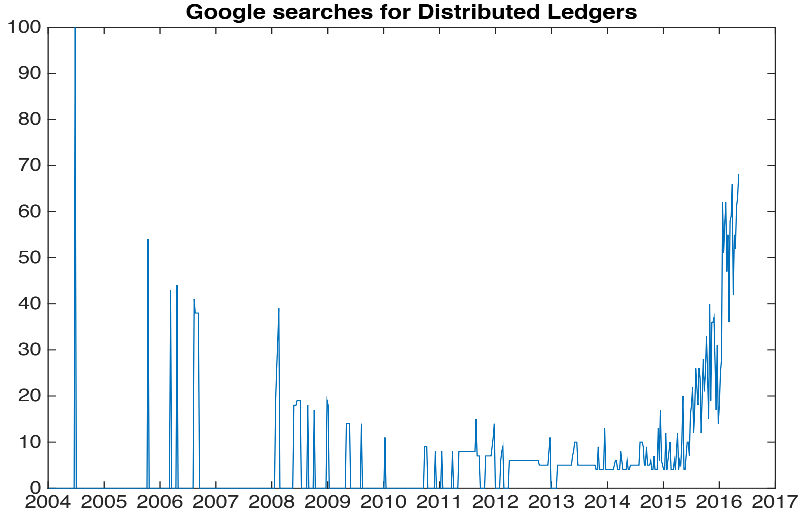


Accounting ledger Europe XIX century

The <u>unalterable</u> ledger?

Clay ledger Mesopotamia 3000BC

The <u>distributed</u> ledger?



The blockchain?

Quipu a blockchain ledger from the Inca Empire

Blockchain technology origins

Hash tree for digital signature - Merkle tree (Ralph Merkle, 1979)

1980

Hash chain for secure login (Leslie Lamport 1981)

1990

e-Cash, first crypto currency, **electronic cash for payments** (David Chaum 1991)

Hash chain for Unix login application with one-time passwords (Neil Haller 1994)

Electronic payments with a hash chain (Thorben Petterson 1995)

1995

n-Count a **hash chain for electronic cash** (Chris Stanform & Eduard de Jong 1995)

ayWord a **hash chain for electronic payments** (Ron Rivest & Adi Shamir 1995)

1997

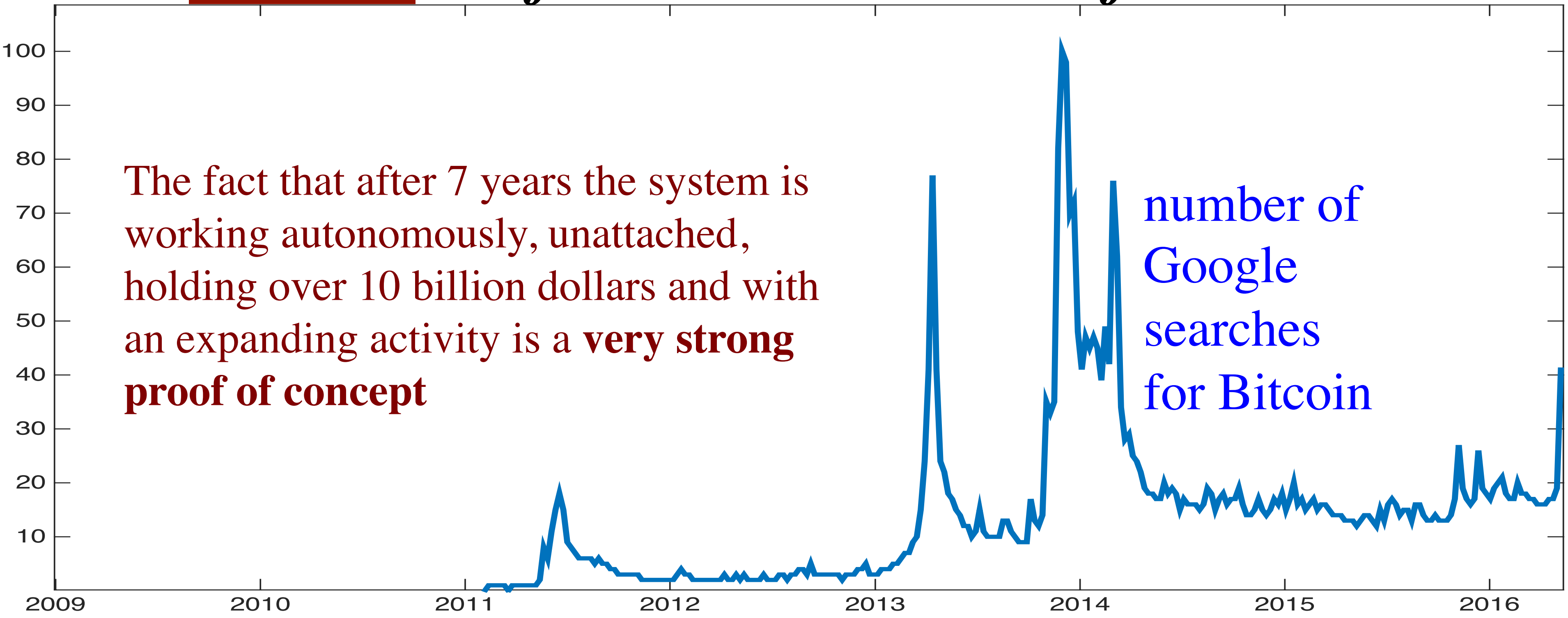
Hashcash – **proof of work** (Adam Back 1997)

2008

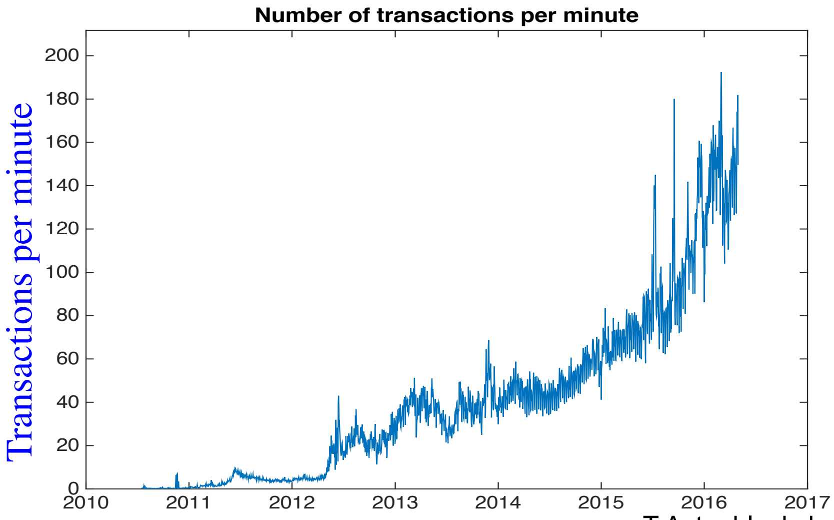
Bitcoin (Satoshi Nakamoto 2008)

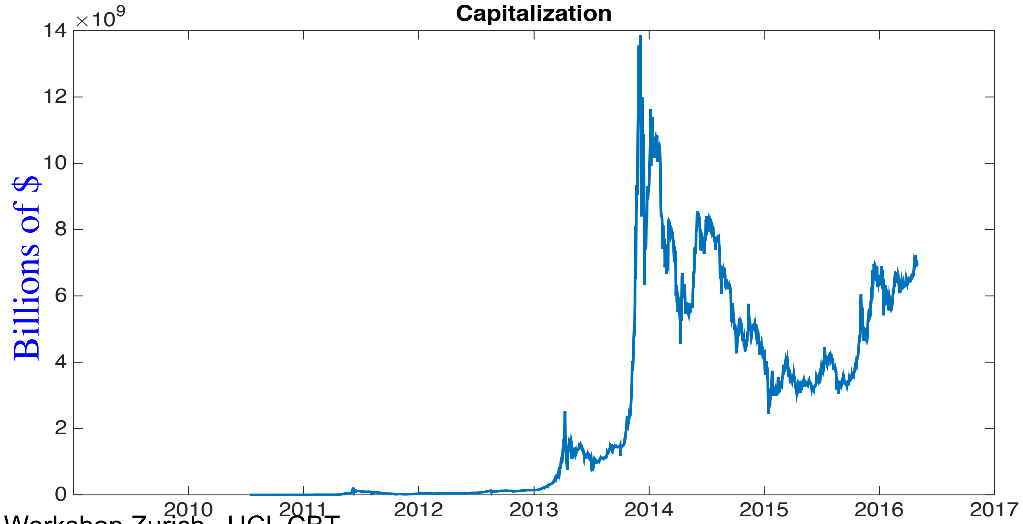
http://networkcultures.org/moneylab/2015/12/15/eduard-de-jong-a-short-history-of-the-blockchain/

Bitcoin itself is the innovation of Bitcoin



The fact that after 7 years the system is working autonomously, unattached, holding over 10 billion dollars and with an expanding activity is a **very strong proof of concept**





Bitcoin hype

Great Expectations

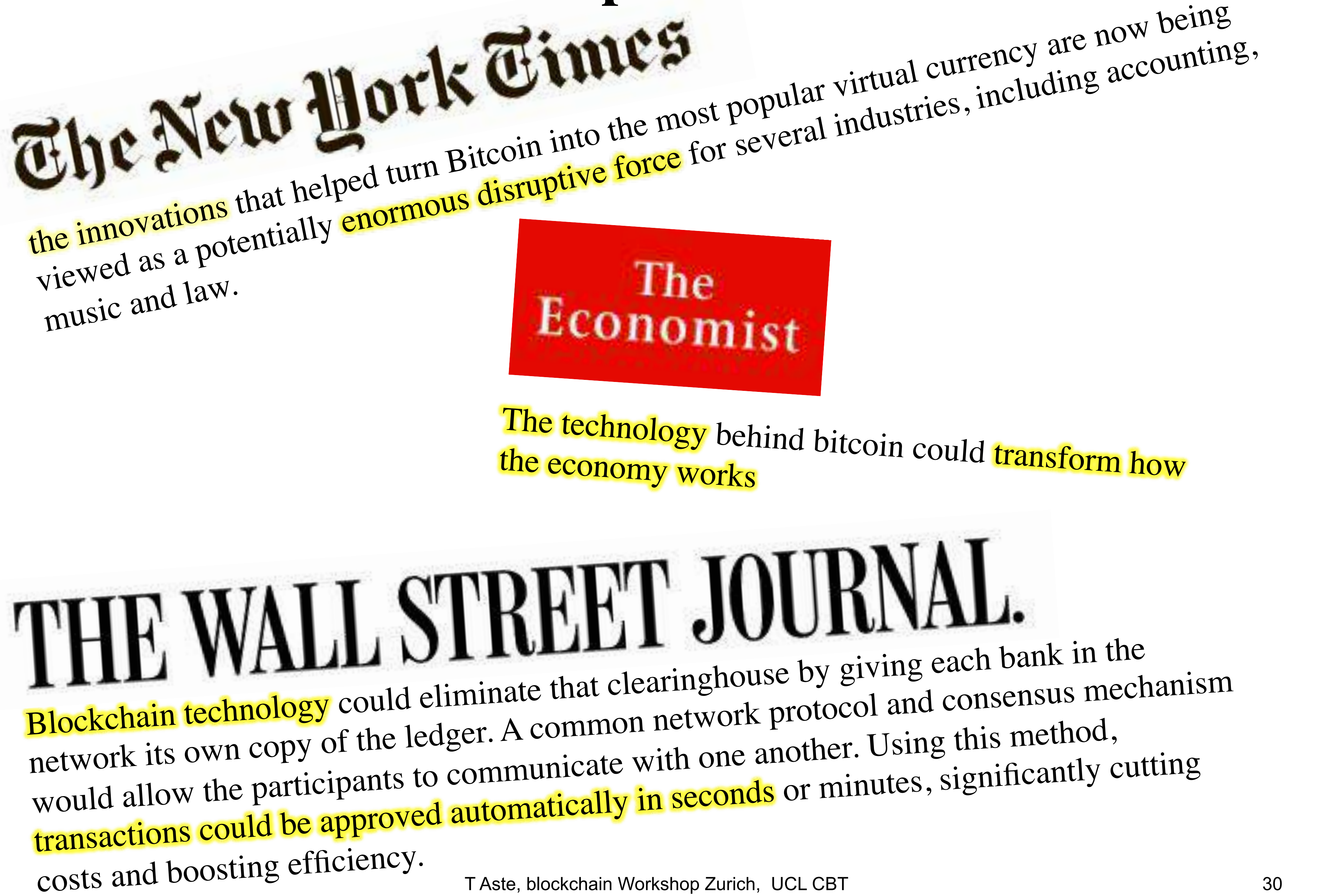
What can actually blockchain can do ?

"While the Bitcoin hype cycle has gone quiet, Silicon Valley and Wall Street are betting that the underlying technology behind it, the **Blockchain**, can change...

…**well everything**"

Goldman Sachs
(December 2015)

Great Expectations



The New York Times

the innovations that helped turn Bitcoin into the most popular virtual currency are now being viewed as a potentially enormous disruptive force for several industries, including accounting, music and law.

The Economist

The technology behind bitcoin could transform how the economy works

THE WALL STREET JOURNAL.

Blockchain technology could eliminate that clearinghouse by giving each bank in the network its own copy of the ledger. A common network protocol and consensus mechanism would allow the participants to communicate with one another. Using this method, transactions could be approved automatically in seconds or minutes, significantly cutting costs and boosting efficiency.

Great Expectations

The Fintech Times

February 2016

TheFintechtimes.com

An independent business newspaper

p. 3

We need to talk about Bitcoin

p. 4

Reinventing money

p. 11

FIntech Industry Outlook

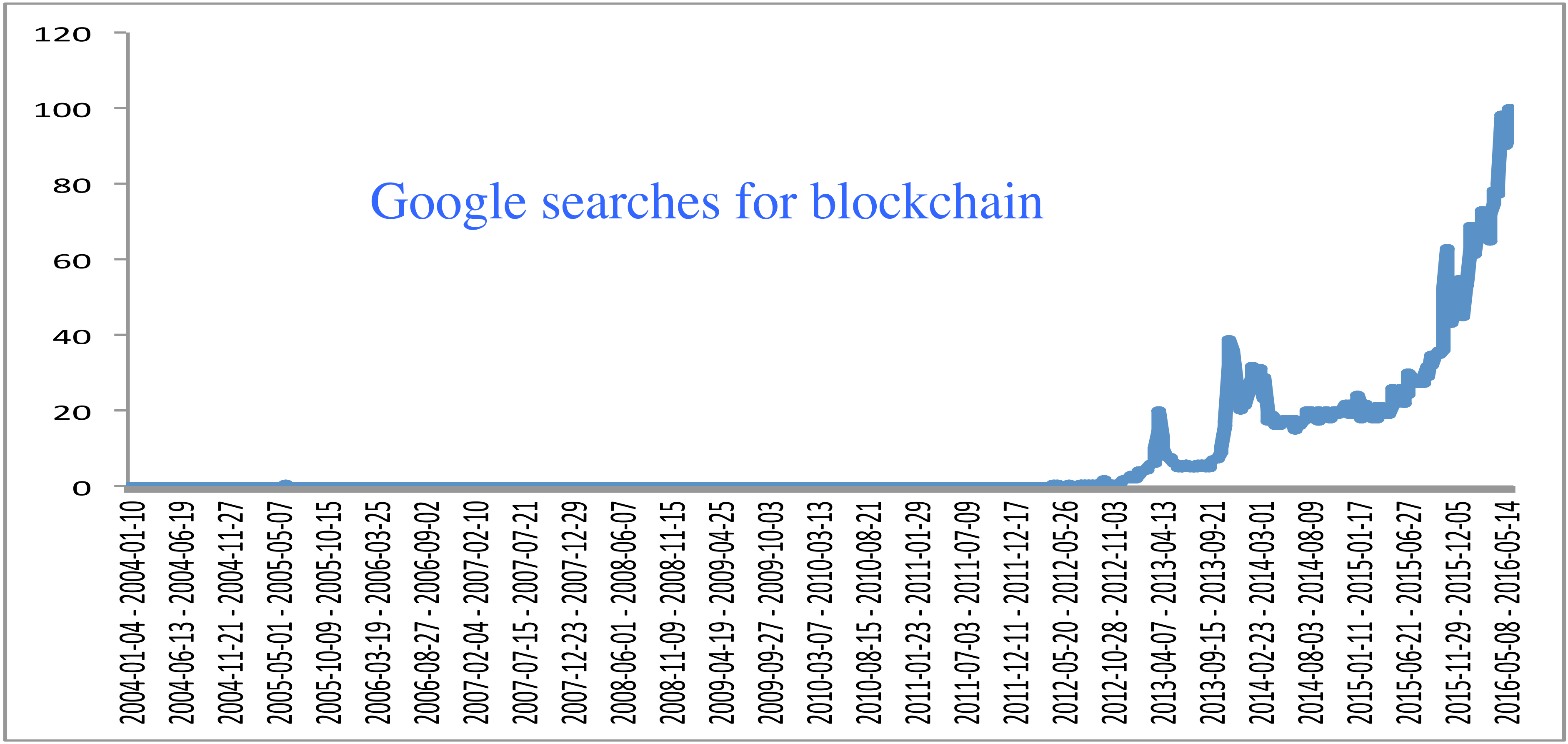
p. 12

Can digital lendig be trusted?

Blockchain, save us!

(p. 3-5)

Bitcoin 2.0


Google searches for blockchain

Blockchain

Global distributed ledger open to anyone

Value (money, titles, deeds, intellectual property, votes…) can be moved and stored securely and privately between un-trustworthy parties

Security is provided by public verification (transparency) and by the unalterable record

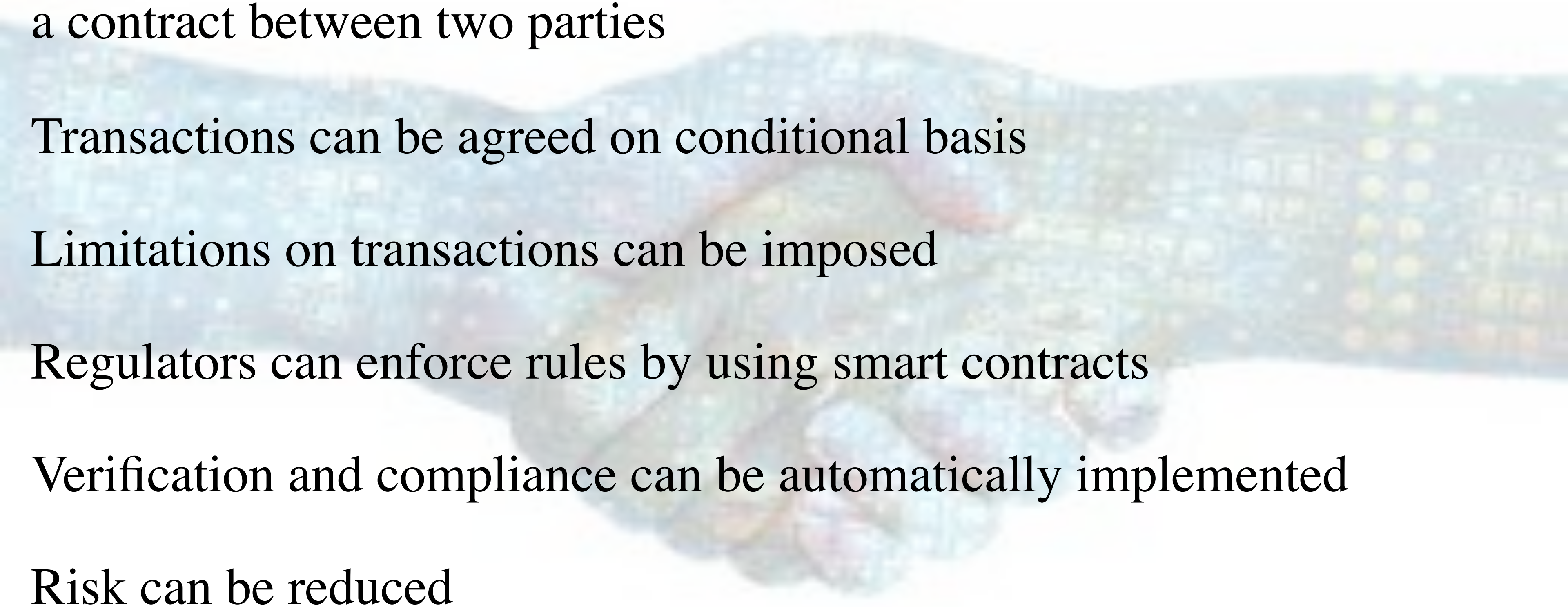
Decentralized reputation systems controlled by the users can become instruments to build new businesses, digital identity associated with reputation can be created

Public access makes compliance with regulations automatically verifiable by anyone (algorithmic regulation)

Machines can operate following smart contracts without need of human supervision generating autonomous organizations

Personal data can be stored, shared and analyzed without being fully revealed with users keeping control

Smart contracts



Computer codes on the blockchain can verify and enforce the terms of a contract between two parties

Transactions can be agreed on conditional basis

Limitations on transactions can be imposed

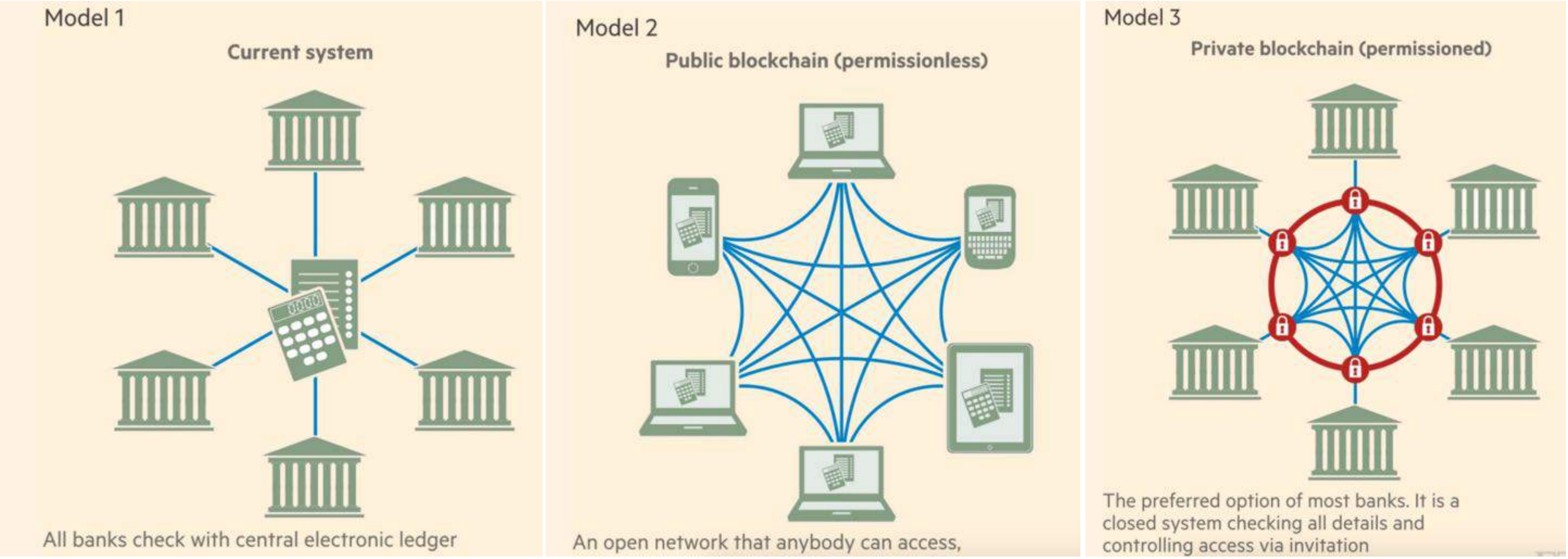
Regulators can enforce rules by using smart contracts

Verification and compliance can be automatically implemented

Risk can be reduced

Combinations of protocols, smart contracts and rules can produce **decentralized autonomous organization** (DAO) that can autonomously operate over the blockchain

Public – Permissioned – Private Blockchains



Model 1

Current system

All banks check with central electronic ledger

Model 2

Public blockchain (permissionless)

An open network that anybody can access,

Model 3

Private blockchain (permissioned)

The preferred option of most banks. It is a closed system checking all details and controlling access via invitation

Source Financial Times 01/11/2015
http://on.ft.com/1k4hrhu

Blockchain: industry impact

Internet of things: Things, humans, money, information and rules can all be in the blockchain that will serve as public ledger for many devices, which would be able to communicate and operate with one another autonomously

Banking: an industry that store and transfer value as blockchain does

Payments: bitcoin has proven the potential of blockchain for money transfer and payments, blockchain can allow unbanked poor to access micro-financial services, changing the world. Smart contracts can condition payments to underlying agreements.

Cyber security: blockchain has proved to be a secure system to transfer value over the Internet

Intellectual property & copyright: blockchain is tracking records form source, open and low cost access allow anyone to have a unique unchangeable proof of existence of a given record at a given time and creators can be directly paid by the users without intermedires

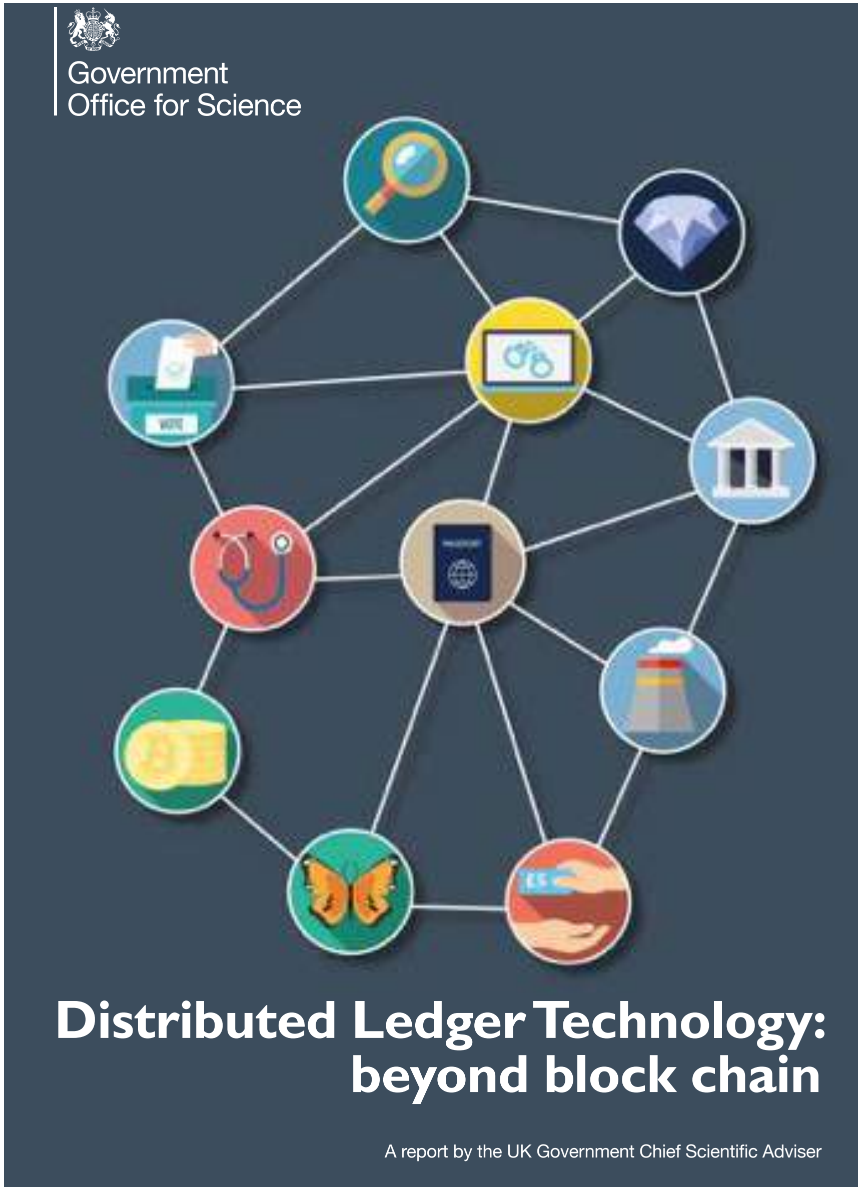
Voting: votes posted into the blockchain cannot be altered or deleted by anyone including the system managers

Contracts & Law: with blockchain smart contracts can be fulfilled automatically, without human intervention.

Taxation: taxes can be applied at the point of sale and then shared across the entire supply chain

Car leasing and sales: driver information, car information and insurance and be matched over the blockchain

Blockchain YES / Bitcoin NO ?



Government Office for Science

Distributed Ledger Technology: beyond block chain

A report by the UK Government Chief Scientific Adviser

Blockchain: limitations

Light travels fast… but pehaps not that fast enough for a fully distributed system that reaches consensus by majority verification....

5,560Km
Greenland
Iceland
Canada
United Kingdom
London
France
Spain
Portugal
New York, NY
United States
North Atlantic Ocean
Mexico
Morocco
Algeria
Libya
Mauritania
Mali
Niger
Chad
Nigeria
Venezuela
Colombia

…. 18.5 ms

Blockchain: risks

Recent history has shown that all technological innovations that started with egalitarian/distributed ethos ended up in high concentration

This is happening already in bitcoin with large concentration of mining activity

Can we prevent this to happen?

Blockchain: governance

Forum Kapitalmarktinstrumente - Kapitalmarktfinanzierung

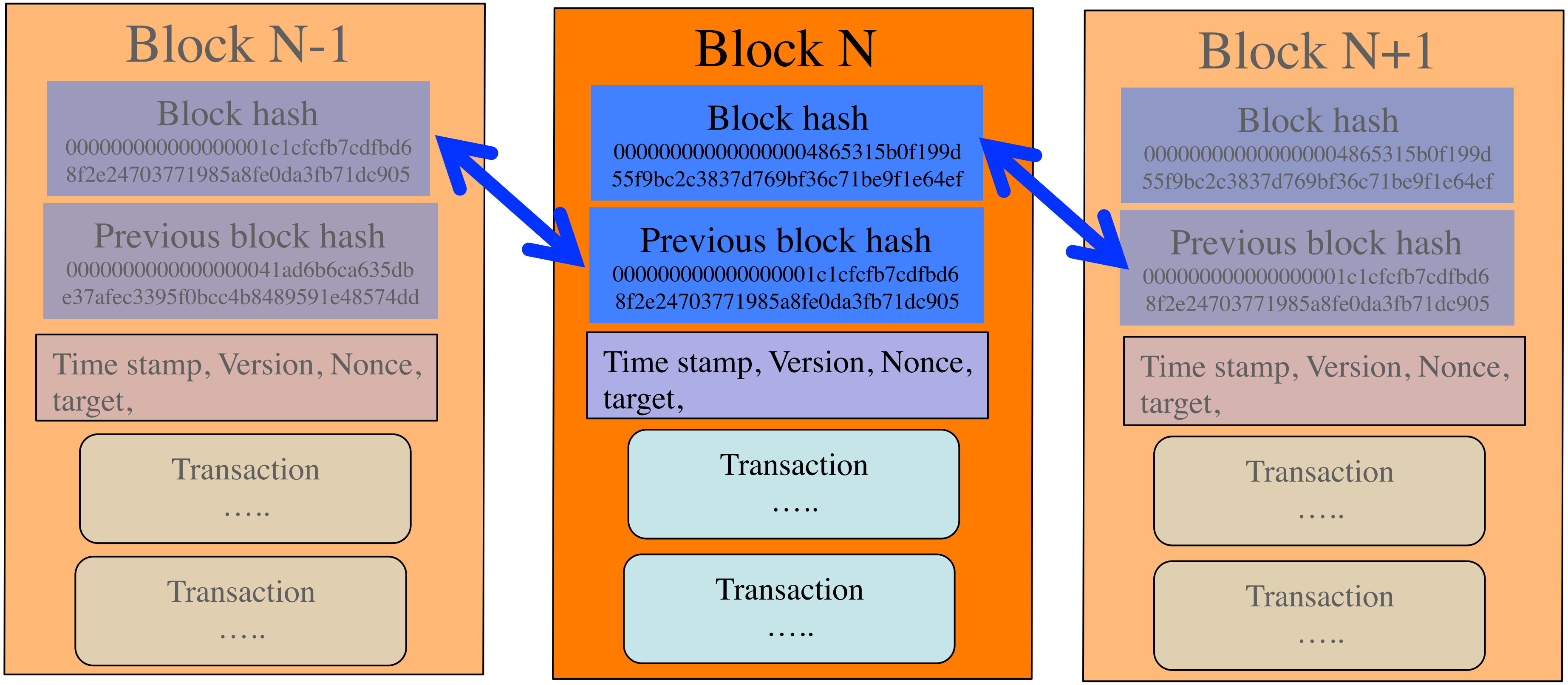
Deutschland | Österreich | Schweiz

Module 2

Blockchain: the next financial Revolution?

– Principles, Opportunities & Risks –

Blockchain



Block N-1

Block hash
000000000000000001c1cfcfb7cdfbd6
8f2e24703771985a8fe0da3fb71dc905

Previous block hash
00000000000000000041ad6b6ca635db
e37afec3395f0bcc4b8489591e48574dd

Time stamp, Version, Nonce, target,

Transaction
…..

Transaction
…..

Block N

Block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

Previous block hash
000000000000000001c1cfcfb7cdfbd6
8f2e24703771985a8fe0da3fb71dc905

Time stamp, Version, Nonce, target,

Transaction
…..

Transaction
…..

Block N+1

Block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

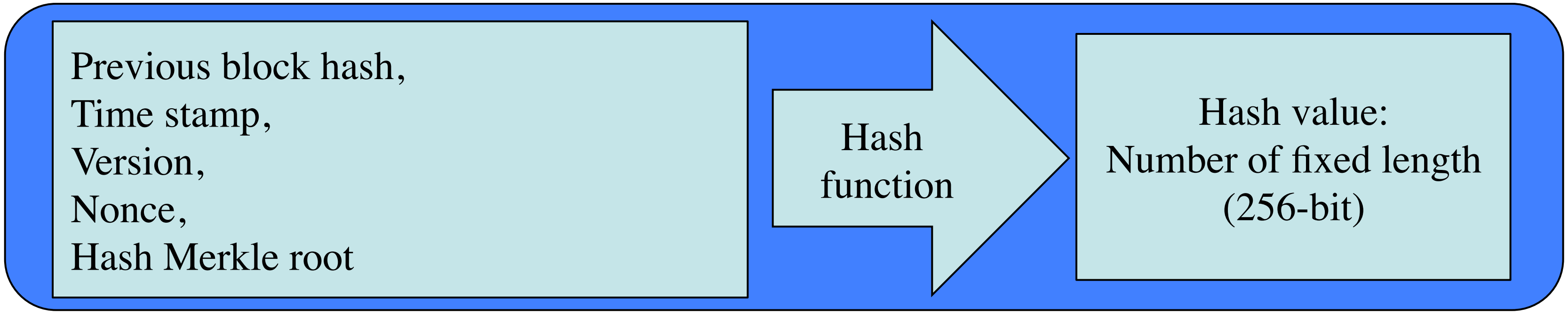
Previous block hash
000000000000000001c1cfcfb7cdfbd6
8f2e24703771985a8fe0da3fb71dc905

Time stamp, Version, Nonce, target,

Transaction
…..

Transaction
…..

Hashing



Previous block hash,
Time stamp,
Version,
Nonce,
Hash Merkle root

Hash function

Hash value:
Number of fixed length
(256-bit)

Blockchain is a Distributed Ledger

Every node in the network has a copy of the blockchain which records all transactions up to the point when the first coin was mined

Transactions are publically announced anyone to verify the authenticity of the data

To avoid double spending, the earliest transaction is the one that counts

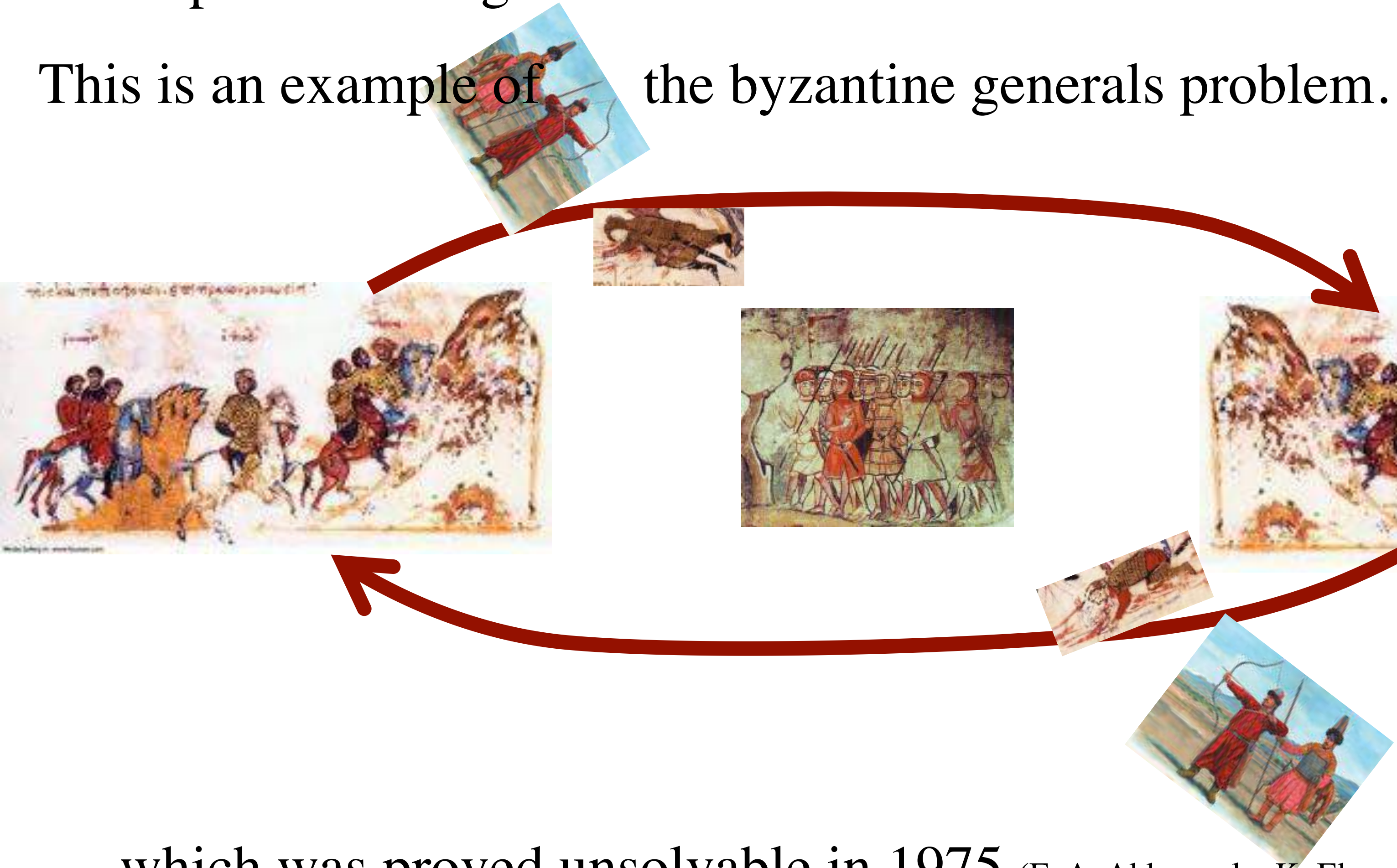
Participants must agree on the order of the transactions

Mining

Blockchain: verification system and agreement

Participants must agree on the ‘true’ content of the blockchain

This is an example of the byzantine generals problem…



… which was proved unsolvable in 1975 (E. A. Akkoyunlu, K. Ekanadham, and R. V. Huber)

In Bitcoin the problem is solved by majority vote

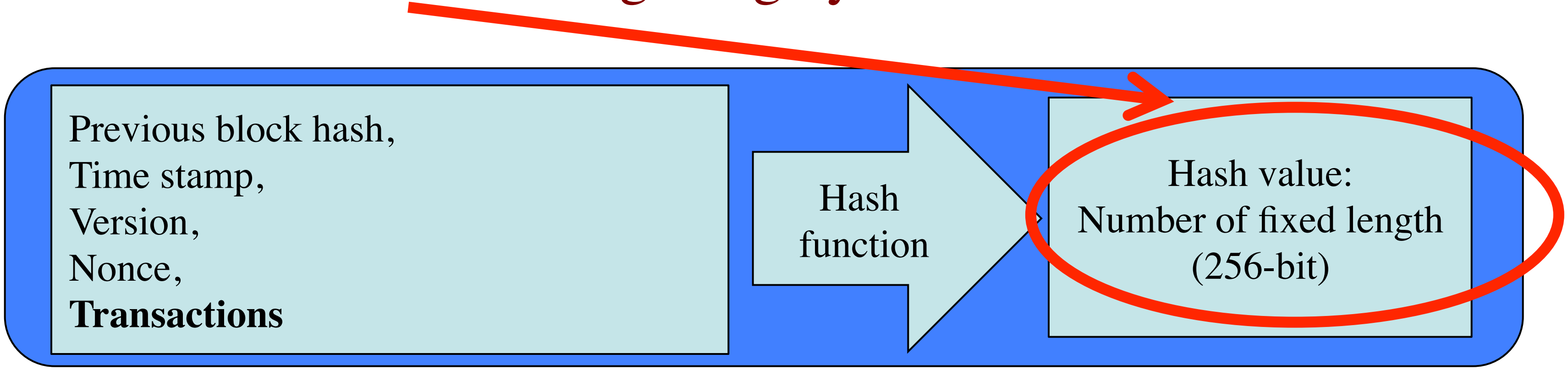
Majority consensus

Truth is what majority believes is true

One CPU one vote

An expensive task is required to users to validate and seal a block. The user that first solve the **proof of work** is compensated with bitcoin (25)

The proof of work requires the hash, generated from the current block content, to be smaller than a certain number, this requires a lot of trials with different *nonce* before getting by chance a valid hash



Previous block hash,
Time stamp,
Version,
Nonce,
Transactions

Hash function

Hash value:
Number of fixed length
(256-bit)

Hashing demonstration

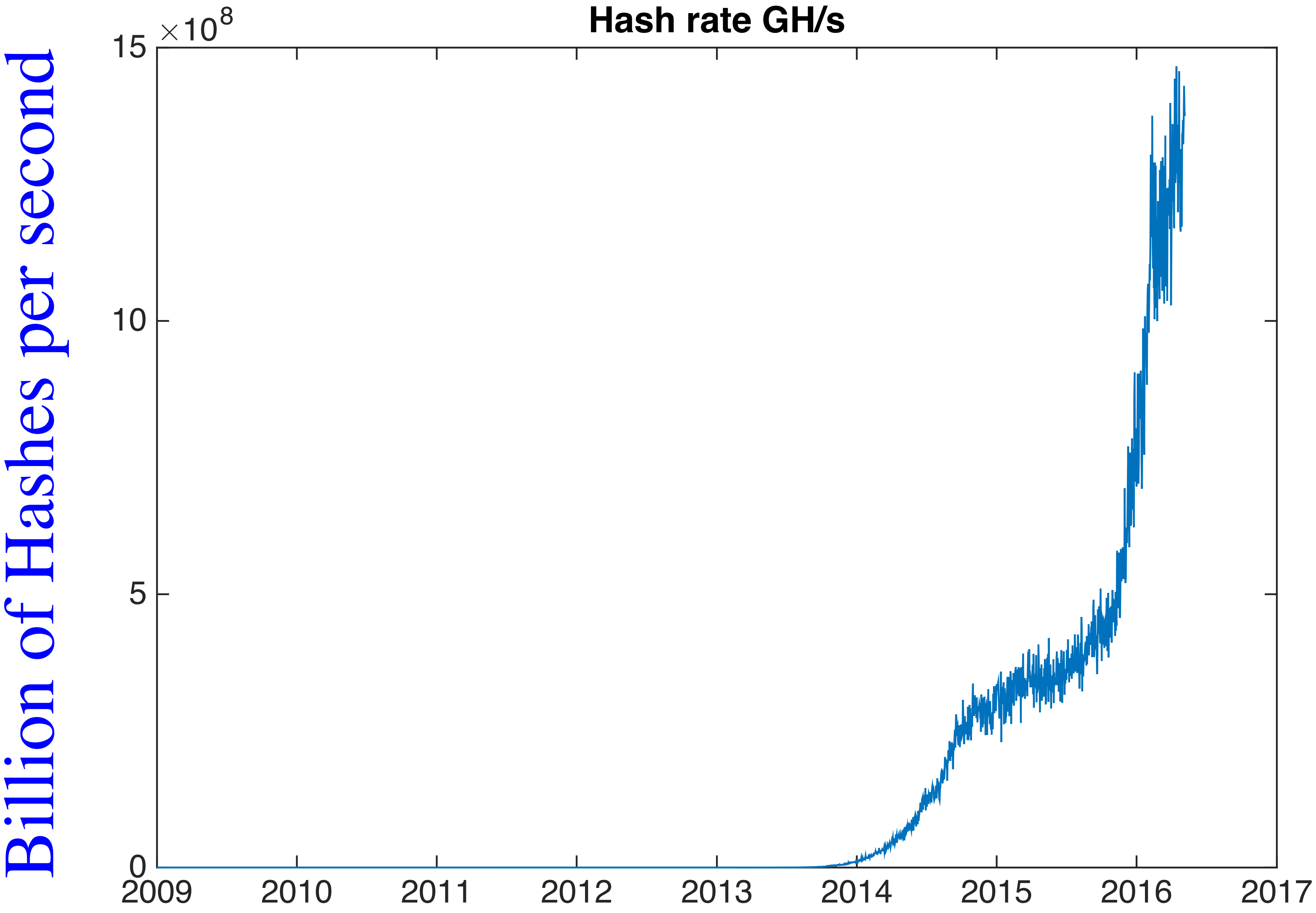
1.46 G G H/ses = 1.46 8 10^{18} H/s

A block header contains these fields:

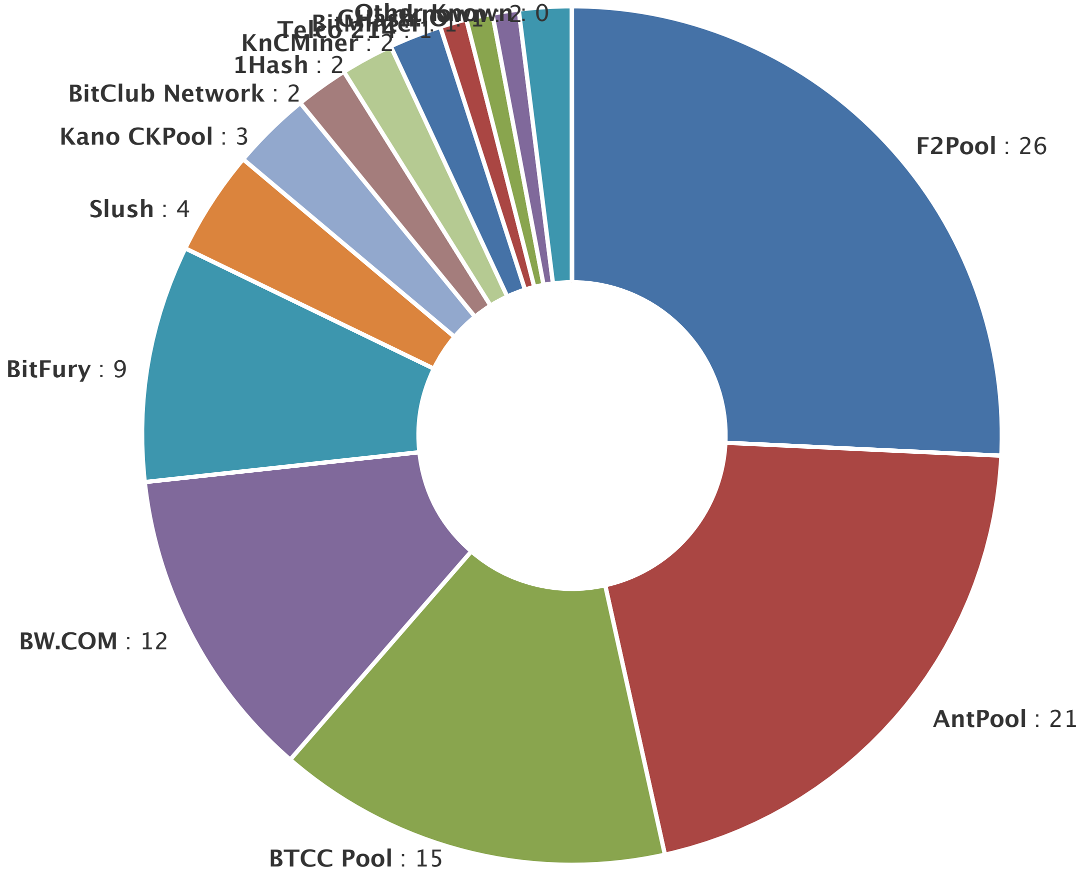
Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	You upgrade the software and it specifies a new version	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4

https://en.bitcoin.it/wiki/Block_hashing_algorithm

Mining activity



Mining concentration

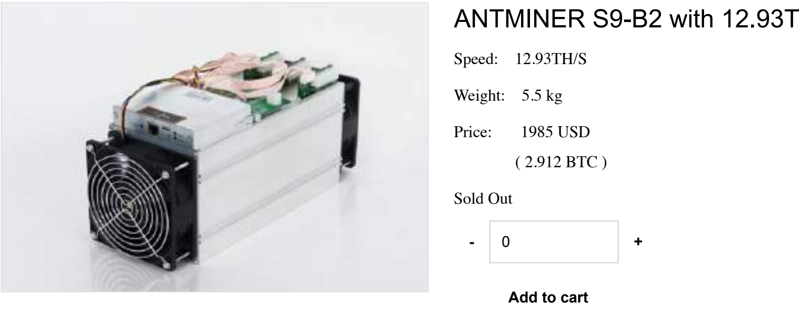


F2Pool	153
AntPool	126
BTCC Pool	91
BW.COM	72
BitFury	54
Slush	22
Kano CKPool	18
BitClub Network	14
1Hash	12
KnCMiner	11
Telco 214	6
BitMinter	4
GHash.IO	3
P2Pool	1
Eligius	1

From: https://blockchain.info/pools

Mining tools

CPU **central processing unit**	0.1 GH/s at 2000 J/GH
GPU **graphics processing unit**	0.5 GH/s at 500 J/GH
FPGA **field-programmable gate array**	10 GH/s at 50 J/GH
ASIC **application-specific integrated circuit**	10,000 GH/s at 0.5 J/GH



ANTMINER S9-B2 with 12.93T

Speed: 12.93TH/S

Weight: 5.5 kg

Price: 1985 USD

(2.912 BTC)

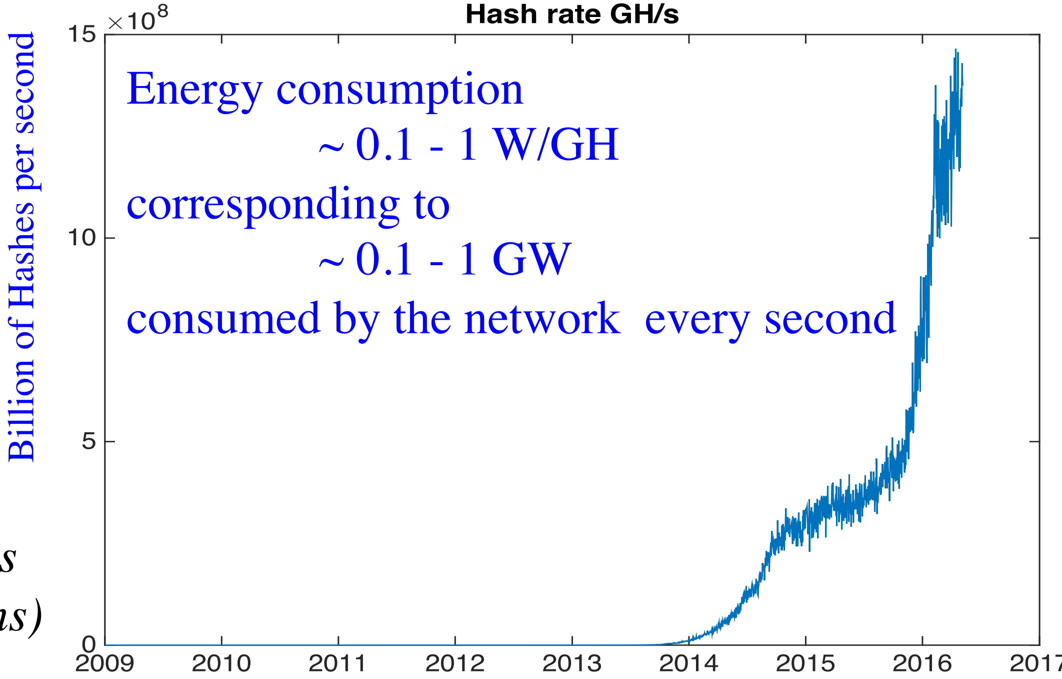
Sold Out

The cost of the proof of work

Bitcoin proof of work is **computationally very costly** it makes too costly to try to alter the transaction history

Globally over one billion of billion hashes per second are generated for the proof of work

*Presently bitcoin network costs **~$5 per transaction** (paid by the miners, the users pay indirectly if they buy and hold Bitcoins) (average transaction volume $500)*



Energy consumption

~ 0.1 - 1 W/GH

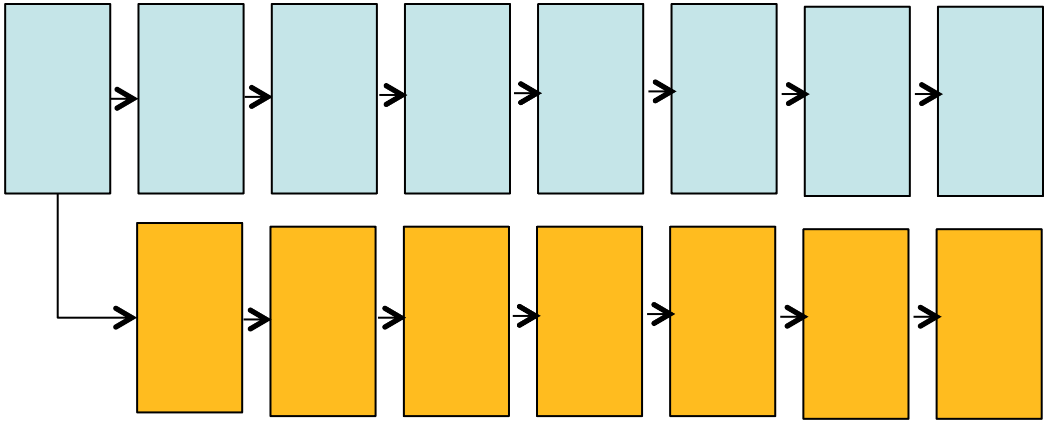
corresponding to

~ 0.1 - 1 GW

consumed by the network every second

Even if the network is holding ~10 billion dollar capitalization it still costs around 10% per year to keep this capital secure

Too costly to attack



block transactions value ~ $1M

chain required length for confirmation = 7

double spending copy

Gain = (block value)

Cost = (proof of work cost) * (chain required length)

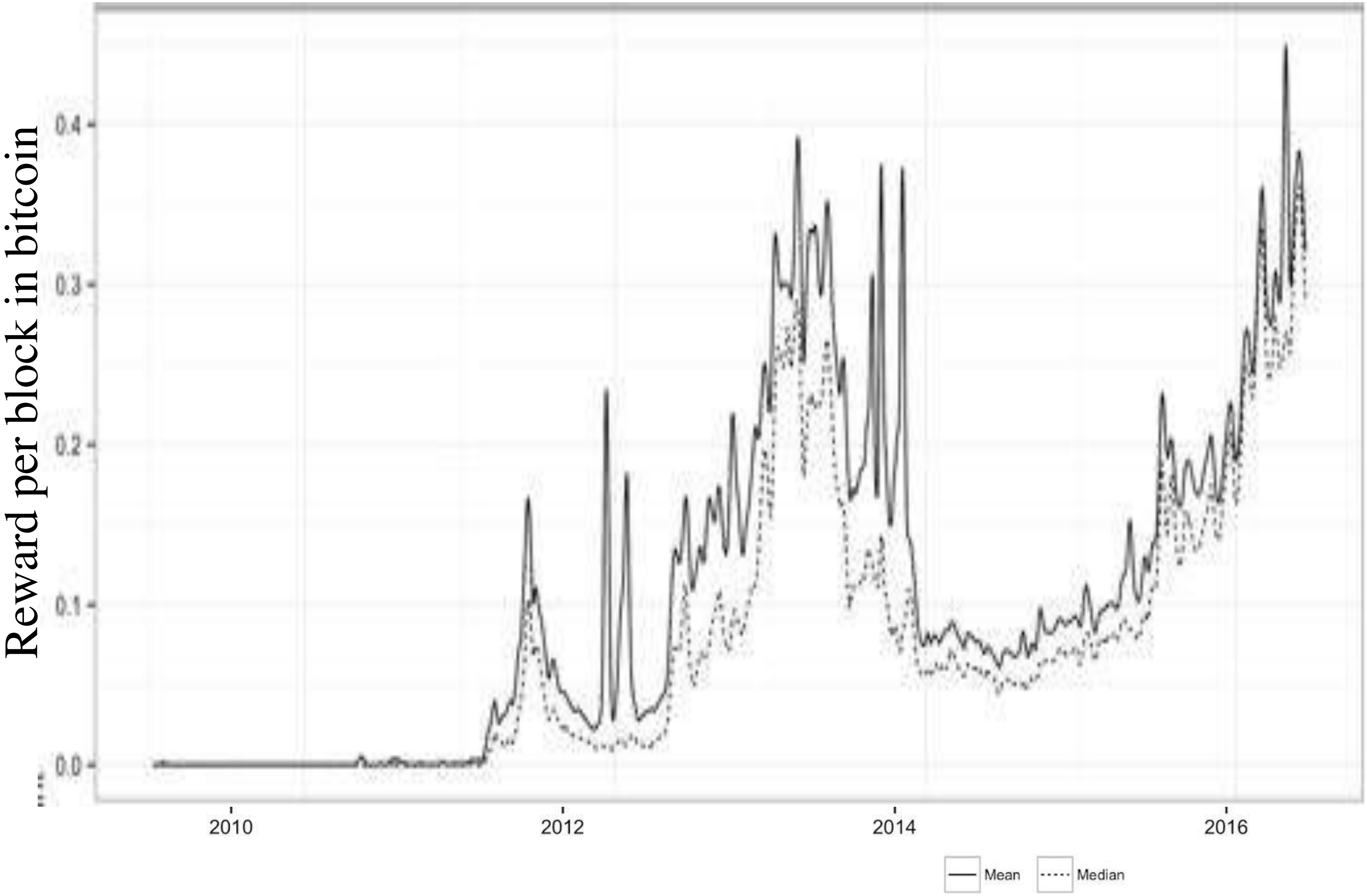
Profit = (block value)-(proof of work cost) * (chain required length)

Profitable if:

(proof of work cost) < (block value)/(chain required length)

Breakeven point: about $100,000

Transaction mining rewards



organofcorti.blogspot.com

The trust machine

The proof of work is the mechanism that produce a blockchain which is verified independently by a large number of participants (miners) that in exchange get a remuneration (25 bitcoins presently ~ $14,000)

This is also the mechanism that creates new coins

The blockchain generates trust because the values exchanged are verified by a large community and the verified recorded history of fair play produces reputation

Unknown, anonymous and untrustworthy parties (even machines) can exchange value

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin could change the world

Alternatives?

Questions?

Thank You

http://blockchain.cs.ucl.ac.uk/