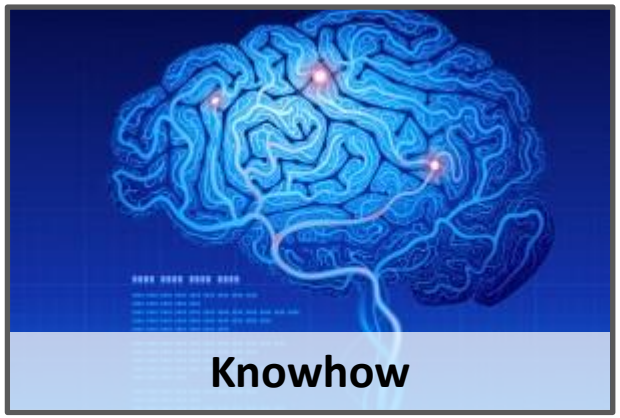
7 Myths
About Bitcoin

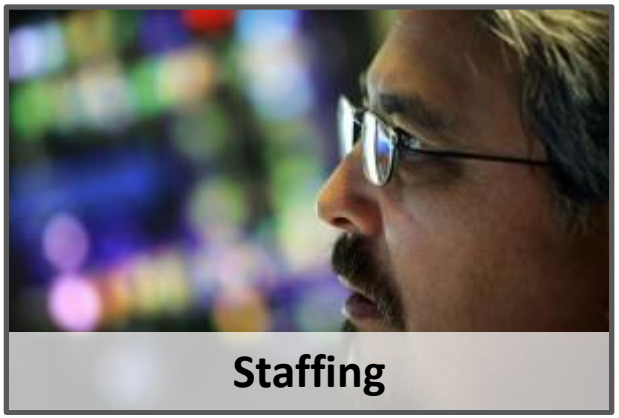
Kristof Verslype
Smals Research

Infosecurity
14 March 2018 - Brussels

Smals

ICT for society





g-cloud

E-gov award
.AGORIA

top EMPLOYER BELGIË BELGIQUE 2017
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

Smals
ICT for society

Why do we study Bitcoin?

- Mainly interested in underlying blockchain technology
- Bitcoin first & most popular blockchain application

What is our impression?

- Sometimes, an inaccurate perception is created

Smals
ICT for society

1 Bitcoin is money

Legal Status in European Union

Ad hoc definition ECB

"A virtual currency is a digital representation of value, not issued by a central bank, credit institution or e-money institution, which in some circumstances can be used as an alternative to money."

Medium of exchange (Ruilmiddel) ?

↳ **Money** ?

↳ **Legal tender (Wettig betaalmiddel)** ✗

↳ **Electronic money** ?

EU - Electronic Money?

European directive 2009/110/EC (Electronic money). Art.2.2

Definition "electronic money"

a) electronically, including magnetically, stored monetary value as represented by a claim on the issuer

b) **issued on receipt of funds** for the purpose of making payment transactions as defined in point 5 of Article 4 of Directive 2007/64/EC

c) which is accepted by a natural or legal person other than the electronic money issuer

According to report of ECB (10/2012) b) not applicable on virtual money such as Bitcoin. Hence, virtual money is not a form of electronic money. Followed by FSMA & NBB (Press release 14/01/2014)

2009/110/EC, article 11: Issuance and redeemability

"Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held."

→ **No guarantee that you can get back the original value** when obtaining the virtual money (**Exchange rate fluctuations**).

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

Legal Status in European Union

Medium of exchange (Ruilmiddel) 

↳ **Money** 

↳ **Legal tender (Wettig betaalmiddel)** 

↳ **Electronic money** 

Money

<u>Legally</u>

Anything widely used to exchange value in transactions

⇒ Degree of acceptance of virtual money is very low

<u>Economically</u>

Should hold 3 properties

1) **Medium of exchange**
2) **Stable store of value**
3) **Unit of account (rekeneenheid)**

⇒ No virtual currency fullfils today these criteria

Bitcoin is not money

Bron: Briefing European Parliament (March 2016): Virtual currencies – Challenges following their introductions

Legal Status in European Union

Medium of exchange (Ruilmiddel) 

↳ **Money** 

↳ **Legal tender (Wettig betaalmiddel)** 

↳ **Electronic money** 

No legal tender
No one obliged to accept payment with virtual currencies

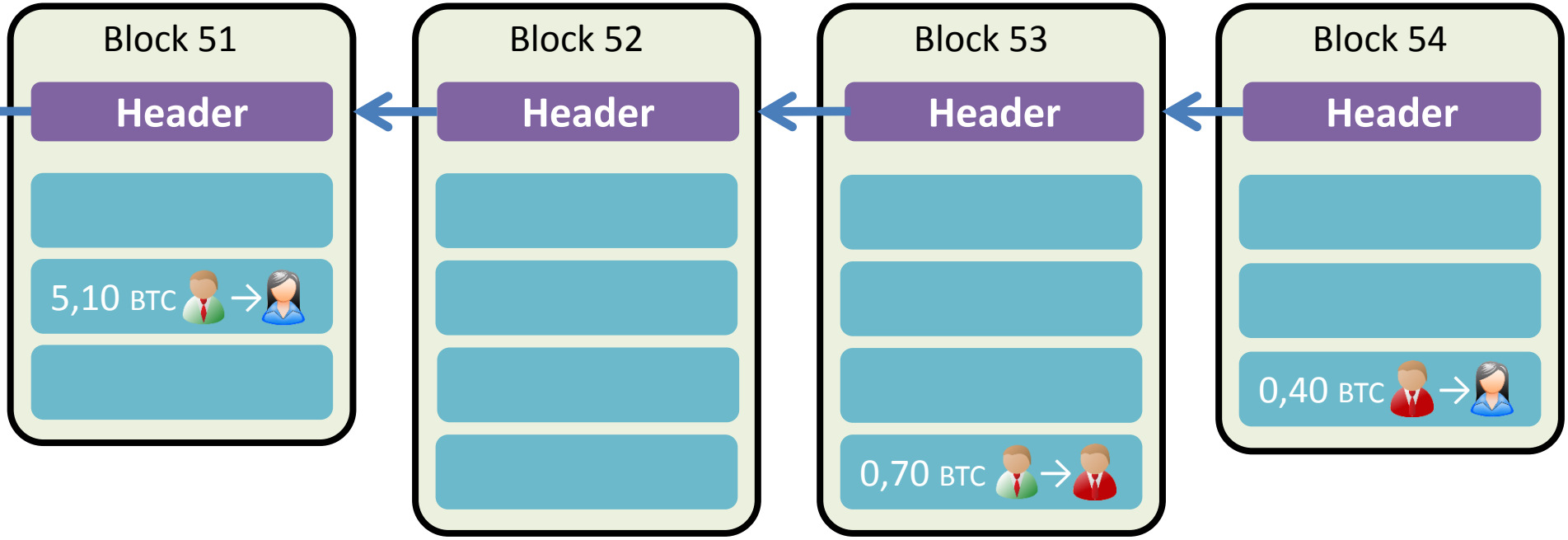
No deposit protection
↔ bank account, term accounts, … (e.g. Legal protection up to € 100 000 by Guarantee Fund)

Not electronic money
No legal guarantee that you will get back the original value (Exchange rate fluctuations)

Smals
ICT for society

2 Bitcoin is efficient

Bitcoin Blockchain



Blockchain = concatenation of blocks, which contain transactions

At predetermined frequency new block appended with most recent transactions

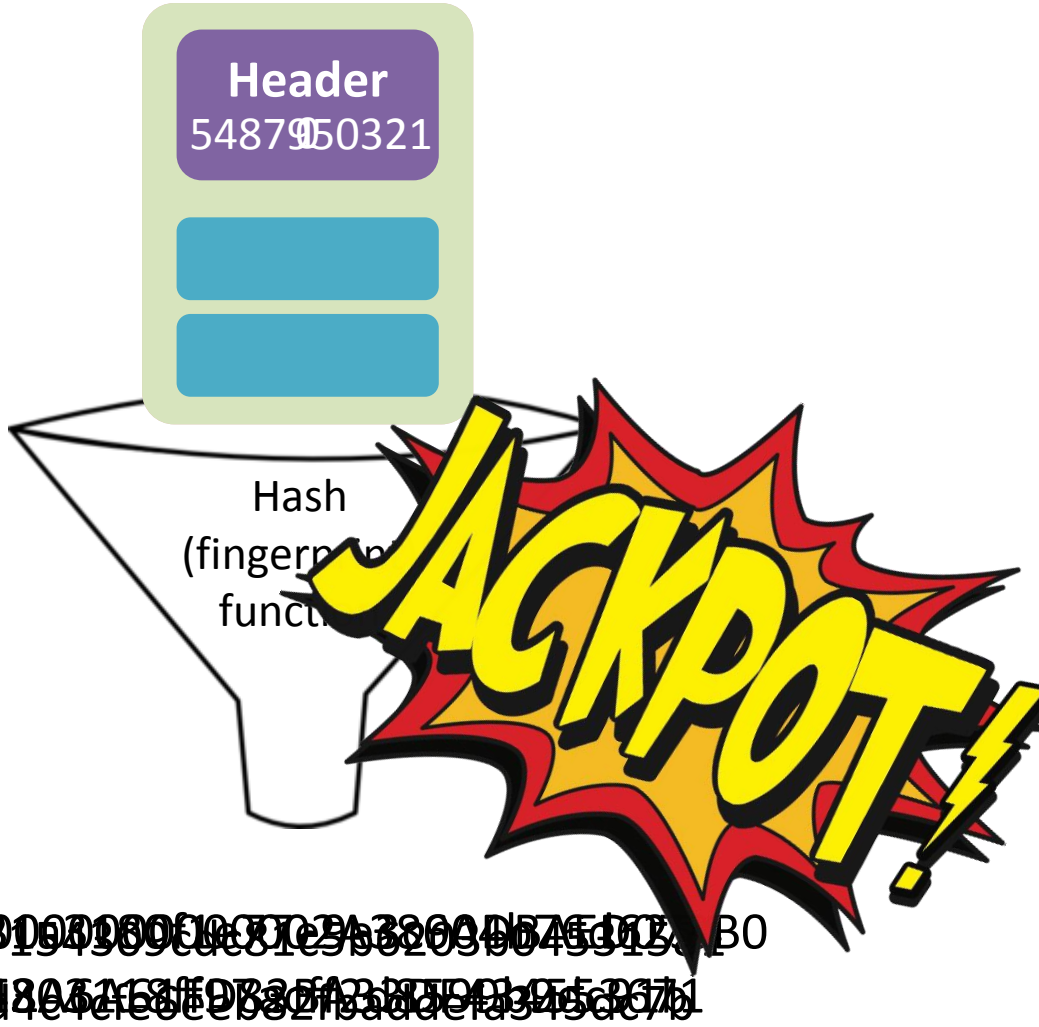
blockchain contains ALL transactions

Transaction in blockchain unremovable & unchangeable

Many entities possess the same copy of the blockchain

Bitcoin Mining

Winner gets reward
- New bitcoins
- Transaction fees



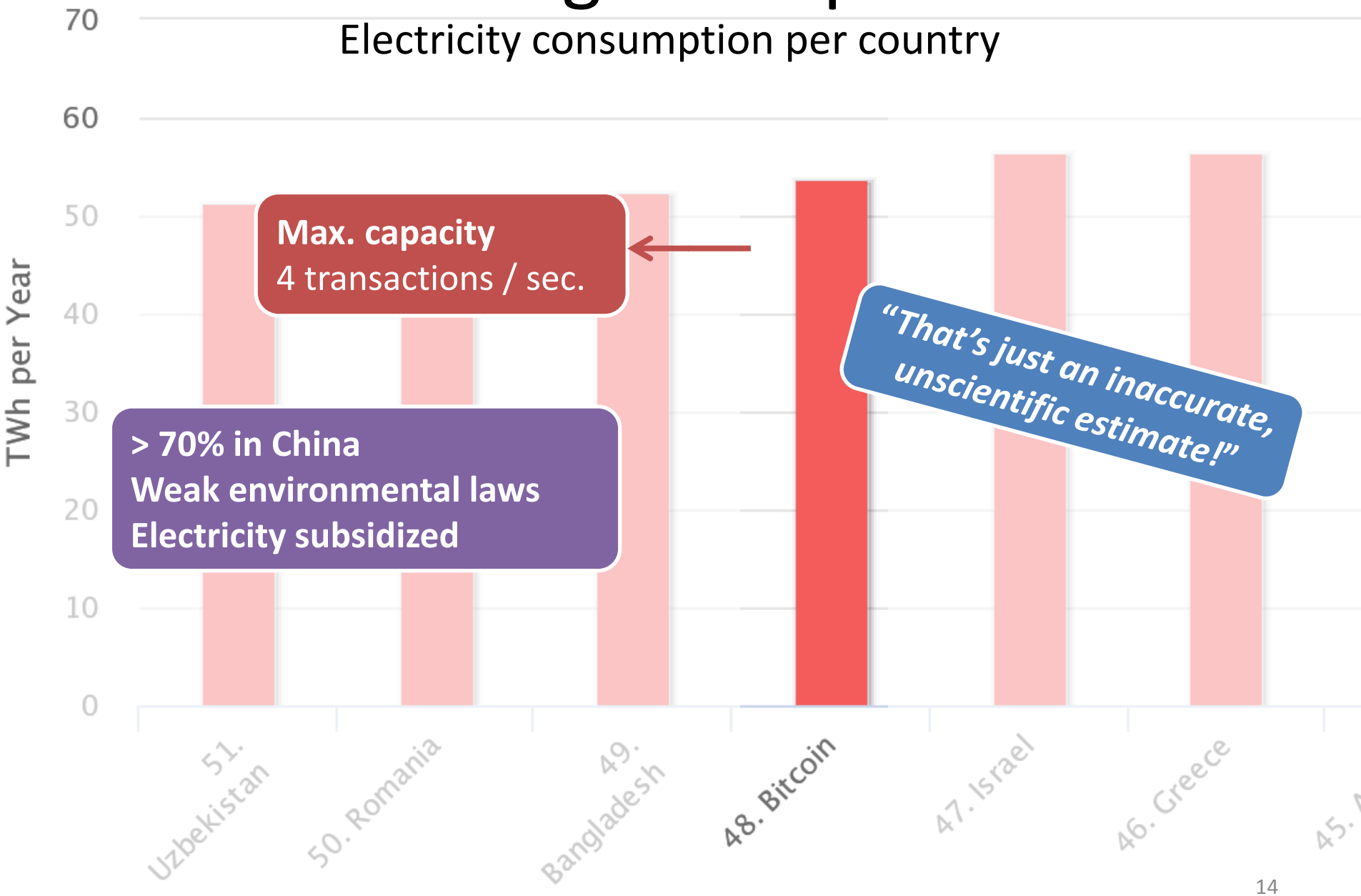
Disclaimer: in reality, only the header is hashed & also random value in coinbase

bitcoin - Mining

Miners compete with each other to solve the cryptographic puzzle of the next block

Ecological Impact

Electricity consumption per country



https://digiconomist.net/bitcoin-energy-consumption

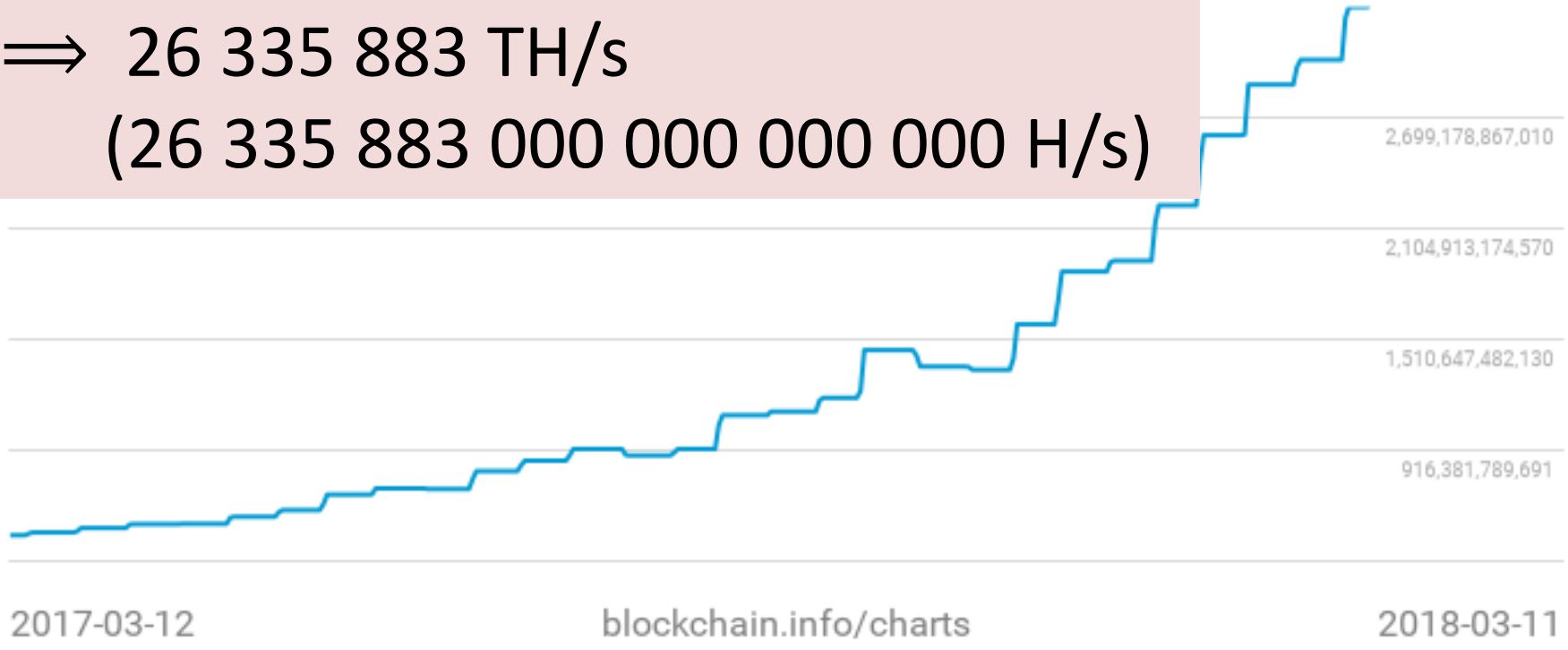
BitcoinEnergyCons

Difficulty

3,290,605,988,755

$\Longrightarrow$ 26 335 883 TH/s

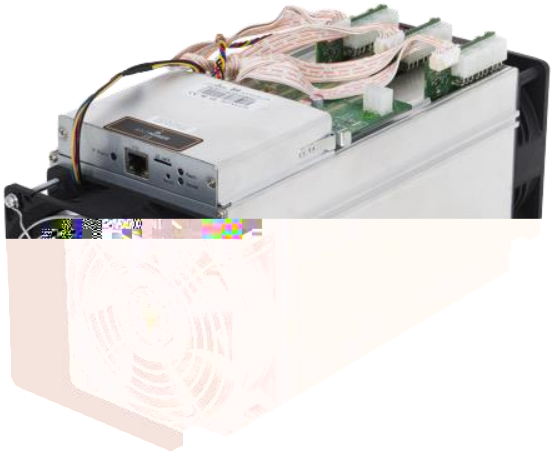
(26 335 883 000 000 000 000 H/s)



Difficulty adjusted every 2 weeks (2016 blocks)

Higher prices → more mining power → higher difficulty

Theoretical Minimum



Antminer S9

- *"Currently the most energy-efficient miner"*
- 14TH/s
- 1323W

26 335 883 TH/s
⟹ 1 881 134 Antminers S9
⟹ 2 488 740 282 Watt
⟹ 21,8 TWh / year
(Excl. cooling)

Belgium
Electricity generation 2016:
82 TWh / year
Electricity consumption 2014:
82 TWh / year

± 11 transactions per Belgian citizen per year

https://www.iea.org/media/countries/Belgium.pdf
https://www.iea.org/publications/freepublications/publication/Energy_Policies_of_IEA_Countries_Belgium_2016_Review.pdf

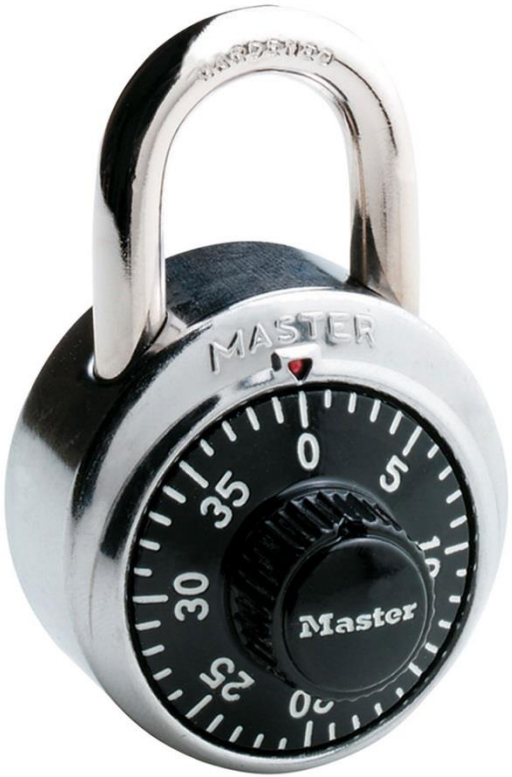
Elimination of trusted authorities (banks)

$\not\Rightarrow$

More efficient

Smals
ICT for society

3 Bitcoin has perfect security



A Sophism…

"Bitcoin already exists 9 years, which proves that it is secure"

Counterexample

WPA2 available since 2004

Proven to be secure

Broken in October 2017

by KU Leuven researchers (KRACK)

Security

Bitcoin is conceptually secure as long as some assumptions are met

Applicative assumptions
E.g. No miner > 50% mining power

Cryptographic assumptions
E.g. SHA-2 & RIPEMD

Mathematical assumptions
E.g. ECDSA

← Heavy assumption

In crypto

- We **trust** that the assumptions are (and stay) correct
- Weaker assumptions → stronger solutions
- Heavier assumptions → weaker solutions

Concentration of Mining Power

The Bitcoin protocol is secure as long as not participant has over 50% of total mining power (*)

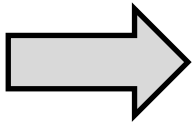
(*) According to Decker and Wattenhofer 49,1% suffices due to stale blocks

There is more than the Blockchain

User

Software

Infrastructure



Loss
Theft
Abuse

James Howells, who works in IT, lost in 2013 7500 bitcoins by throwing away by accident an old hard disk, which contained his secret key.

Nearly 4M Bitcoins Lost Forever

Source: chainalysis.com

Risk

Central entity → individual user

bitcoin

Withdraw limit	✓	X
Card stop	✓	X
Refund	✓	X
Deal with loss	✓	X

→ Sometimes, we are happy that there is a central party...

https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/?mbid=nl_102917_daily_list1_p1

Online Wallets

Online wallet

Manages your bitcoins
Full trust required

Some hacked online wallets…

PicoStocks.com
MT.GOX
Bter.com
mintpal
linode
BITFINEX
nicehash
bithumb
Inputs.io
BITSTAMP
SECURE TRADING AND MONEY PAYMENT
Coincheck
支払いを、もっと便利に、快適に
比特币存钱罐

Customers lost money

Thu 7 Dec '17 10.38 GMT

theguardian

Bitcoin: $64m in cryptocurrency stolen in 'sophisticated' hack, exchange says

perates with words

Mining marketplace NiceHash suspends operations while it co-op authorities over 'professional attack', urging users to change pass

Nearly $64m in bitcoin has been stolen by hackers who broke into Slovenian-based bitcoin mining marketplace NiceHash.

The marketplace suspended operations on Thursday while it investigated the breach, saying it was working with law enforcement as "a matter of urgency" while urging users to change their passwords.

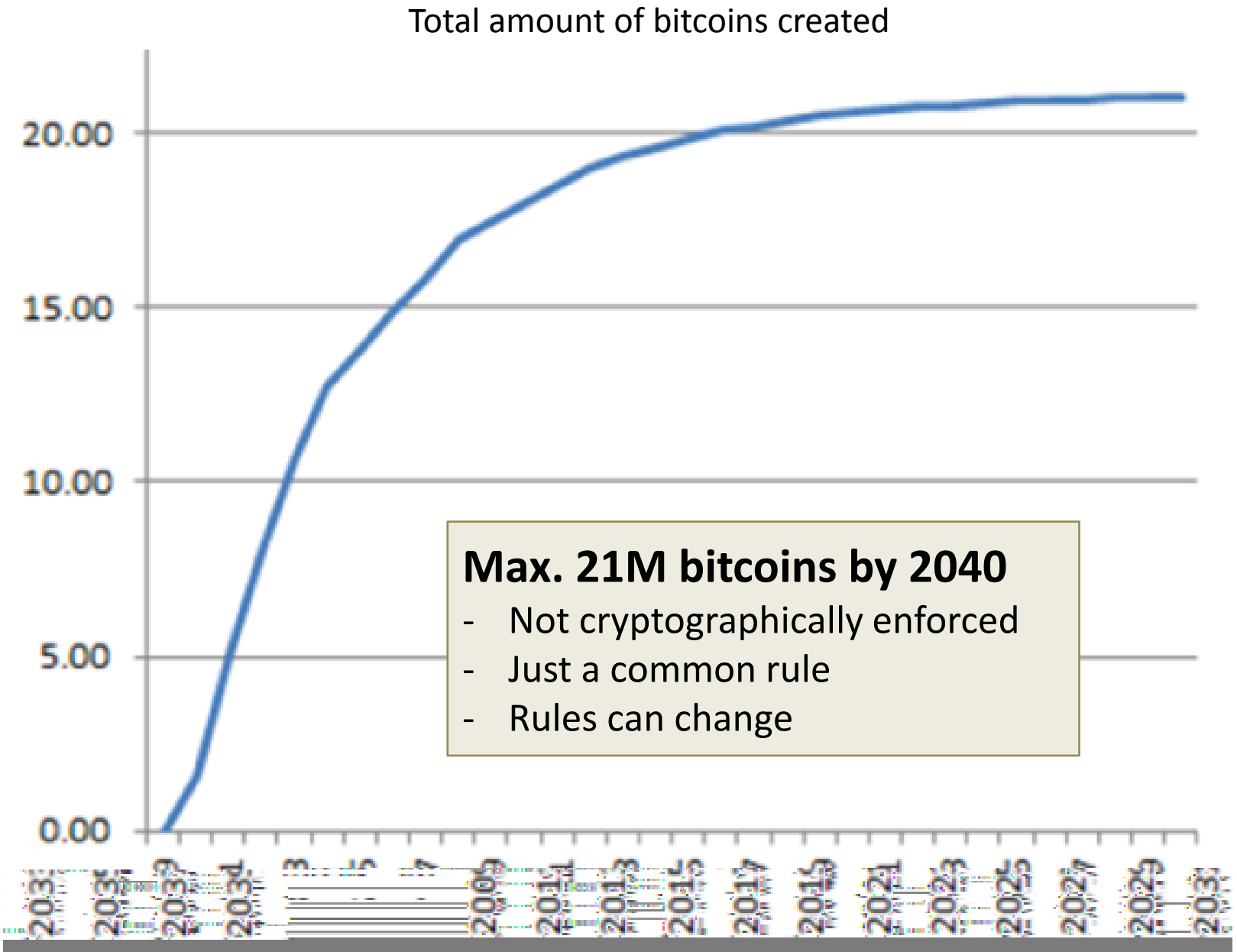
The hack was "a highly professional attack with sophisticated social engineering" that resulted in approximately 4,700 bitcoin being stolen, worth about $63.92m at current prices, said NiceHash head of marketing Andrej P Škraba.

https://www.theguardian.com/technology/2017/dec/07/bitcoin-64m-cryptocurrency-stolen-hack-attack-marketplace-nicehash-passwords

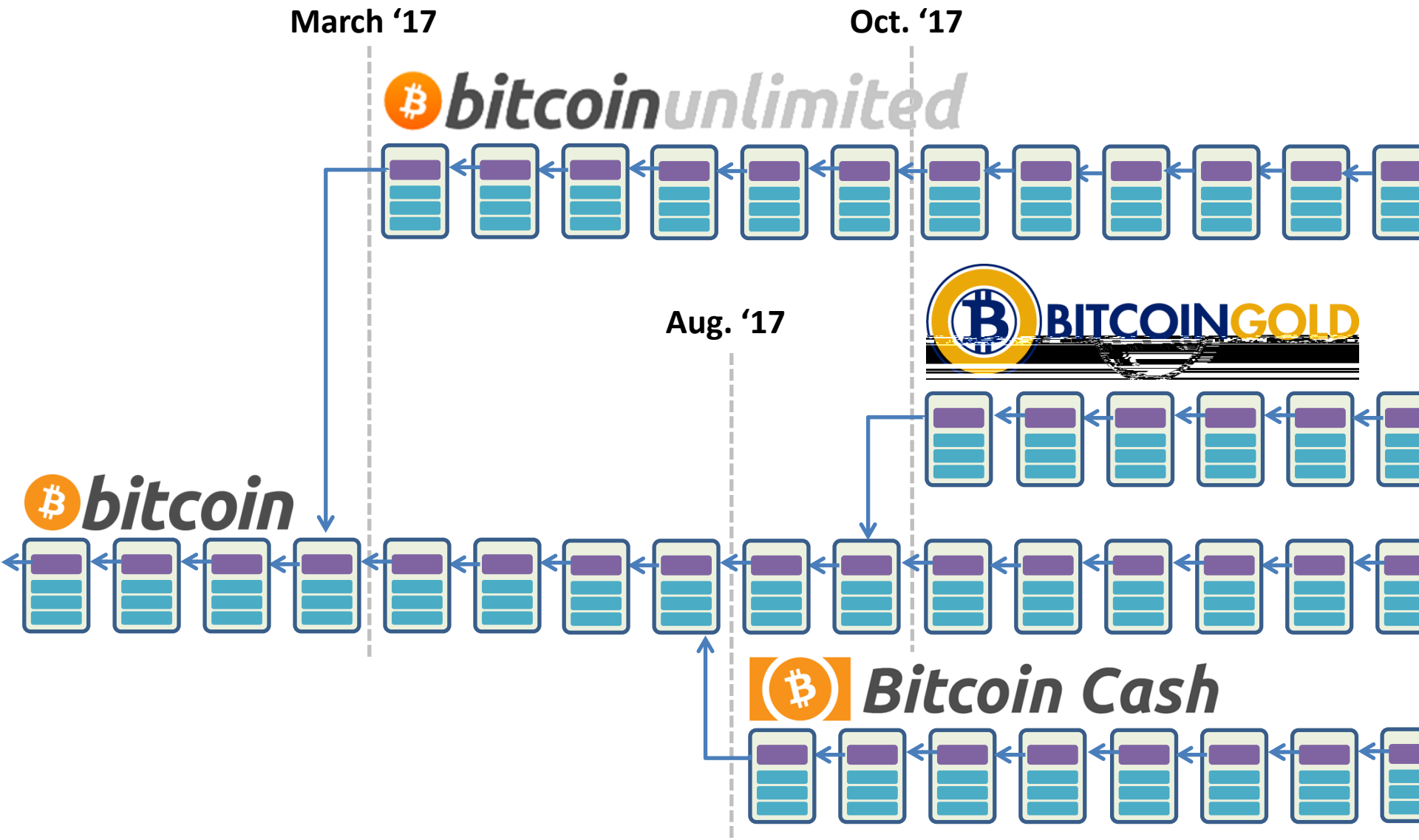
Smals
ICT for society

4 Bitcoin is a scarce asset, like gold

Total Amount of Bitcoins

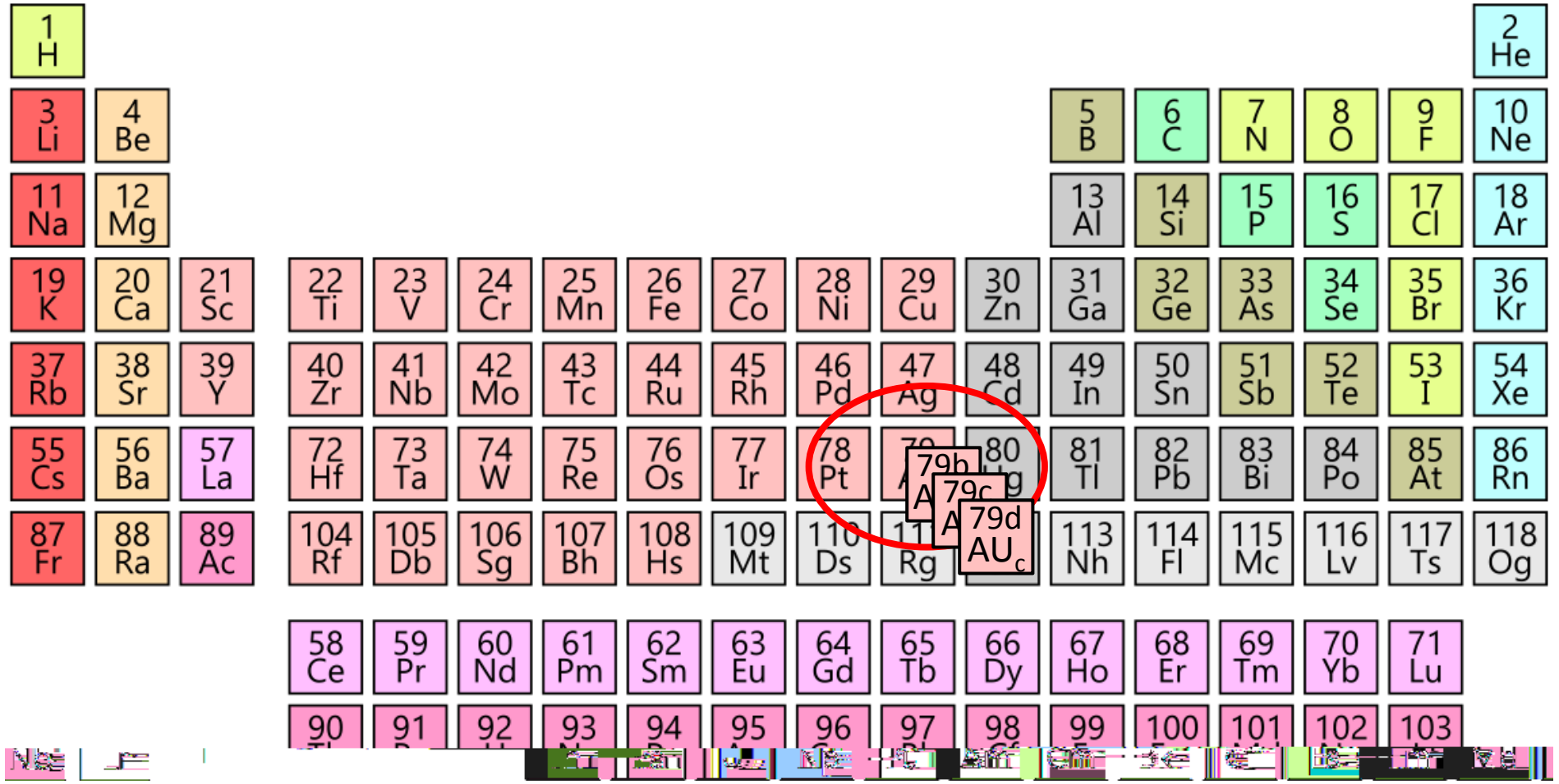


Forks


March ‘17
Oct. ‘17
bitcoinunlimited
Aug. ‘17
BITCOINGOLD
bitcoin
Bitcoin Cash

Periodic Table

(Table of Mendelejev)



Altcoins

#	Name	Symbol	Market Cap	Price	Circulating Supply	V
1	Bitcoin	BTC	$181.214.836.784	$10.729,70	16.889.087	$
2	Ethereum	ETH	$87.551.820.315	$894,56	97.871.925	$
3	Ripple	XRP	$37.735.632.299	$0,965234	39.094.802.192 *	
4	Bitcoin Cash	BCH	$22.011.418.650	$1.295,56	16.989.888	
5	Litecoin	LTC	$12.341.360.446	$222,77	55.400.308	$
6	NEO	NEO	$9.371.440.000	$144,18	65.000.000 *	
7	Cardano	ADA	$8.790.262.141	$0,339038	25.927.070.538 *	
8	Stellar	XLM	$6.810.062.729	$0,368748	18.468.066.889 *	
9	IOTA	MIOTA	$5.308.430.320	$1,91	2.779.530.283 *	
10	Dash	DASH	$5.078.204.941	$642,08	7.908.954	
11	Monero	XMR	$4.834.894.443	$306,63	15.767.794	

coinmarketcap.com

887	InvisibleCoin	IVZ	$?	$0,376429	? *	$6
888	CoffeeCoin	CFC	$?	$0,003427	? *	$5
889	Moneta	MONETA	$?	$0,000428	?	$5
890	The Vegan Ini...	XVE	$?	$0,000750	? *	$4
891	FutCoin	FUTC	$?	$0,003213	?	$4
892	Cheapcoin	CHEAP	$?	$0,000643	? *	$3
893	Dashs	DASHS	$?	$0,042944	?	$3
894	Dubstep	DUB	$?	$0,002677	? *	$3
895	PrismChain	PRM	$?	$0,002249	? *	$1
896	GameLeagueCoin	GML	$?	$0,018128	? *	$0
897	AvatarCoin	AV	$?	$0,063798	? *	$0
898	International...	XID	$?	$0,004152	?	$0
899	FrankyWillCoin...	FRWC	$?	$0,003405	?	$0

Each creation of a succesful crypto currency ~ creation of new, rare, element on the periodic table (but with different properties)

	?				$?	$0,005377
	? *				$?	$0,000102
	?	$?	902	OCOW	OCOW	$? $0,000017

Just a rule

Forks

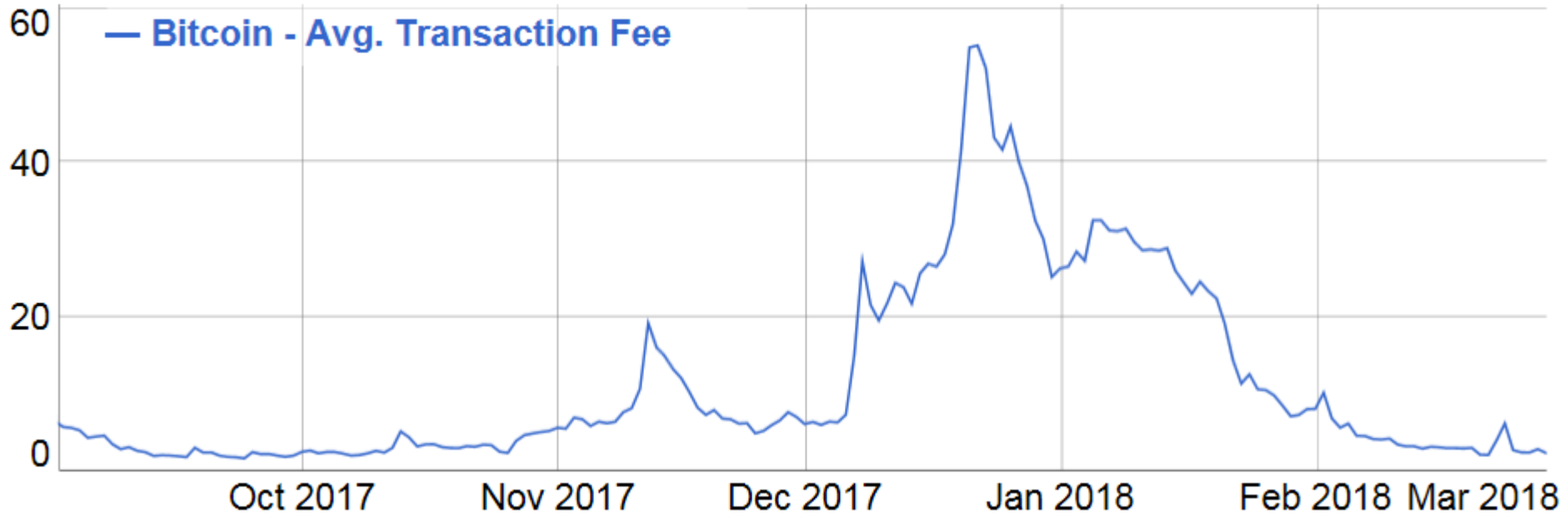
Altcoins

Supply of crypto currencies theoretically unlimited

Smals
ICT for society

5 Bitcoin has low transaction fees

Average Transaction Fee in $



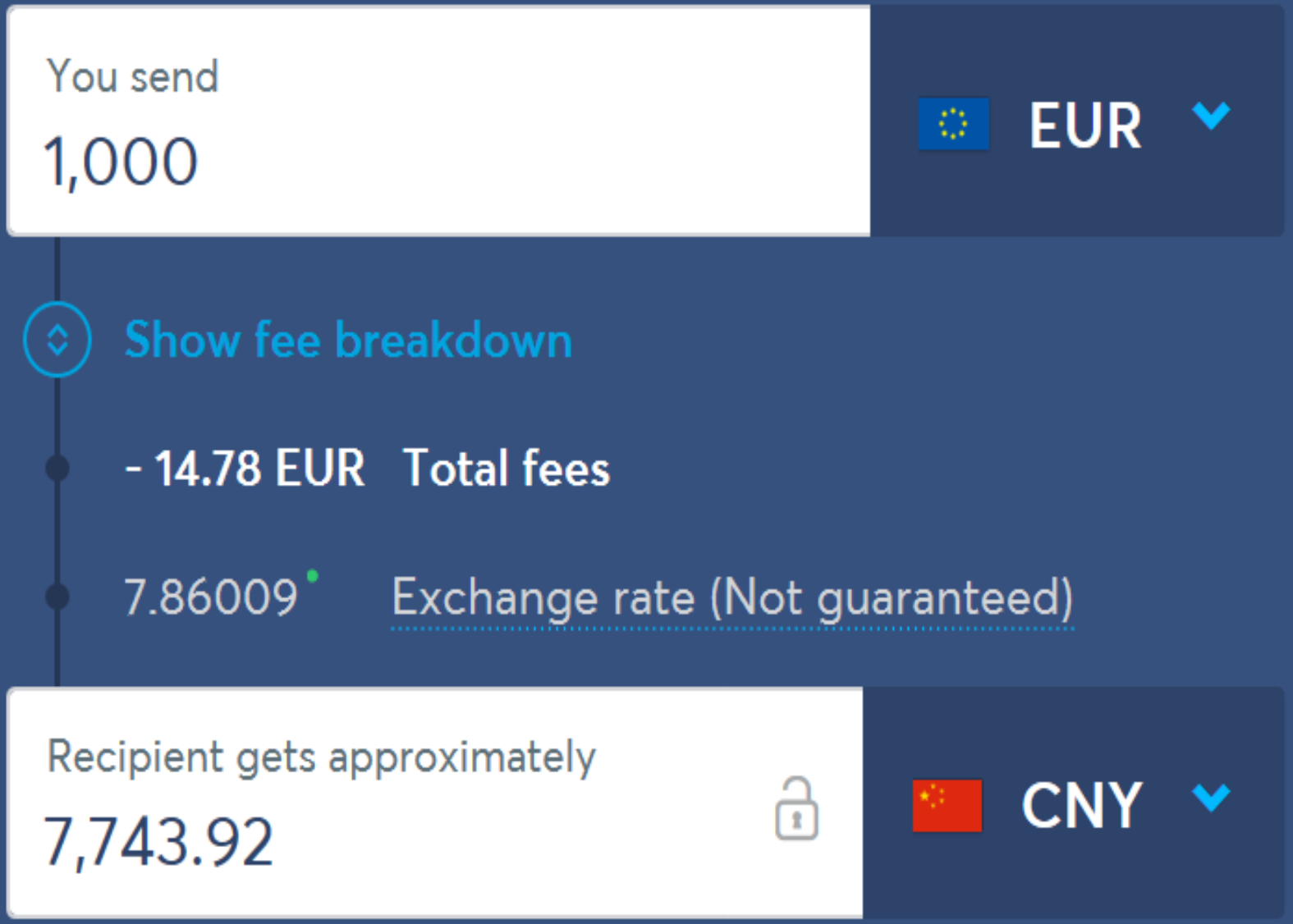
Volatile & unpredictable

Based on supply & demand

Based on size (in bytes) of transaction, not on amount

Payed by the entity sending money

https://bitinfocharts.com/comparison/bitcoin-transactionfees.html#1y


You send
1,000
EUR
Show fee breakdown
- 14.78 EUR Total fees
7.86009
Exchange rate (Not guaranteed)
Recipient gets approximately
7,743.92
CNY
Should arrive in 27 minutes

Bitcoin is not always the cheapest option

Smals
ICT for society

6 Bitcoin is anonymous

One-Time Pseudonyms

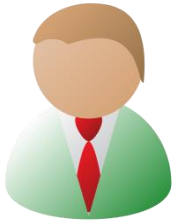
Better privacy

Physical world

Bitcoin network

Bob

Alice



Charlie

Transaction

0,8 BC →

0,4 BC →

Bitcoin & Privacy

Degree of privacy on Bitcoin network, but far from perfect

PRINCETON UNIVERSITY

"We show that, if the user pays using a cryptocurrency, trackers typically possess enough information about the purchase to uniquely identify the transaction on the blockchain, link it to the user's cookie, and further to the user's real identity.

Massachusetts Institute of Technology

"Identified" persons linked to

WikiLeaks

satoshiDICE!
over 98% breakeven odds

Silk Road
anonymous marketplace

Fleder, Michael, Michael S. Kester, and Sudeep Pillai. MIT. "Bitcoin transaction graph analysis." *arXiv preprint arXiv:1502.01657* (2015).
Goldfeder, Steven, et al. "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies." arXiv preprint arXiv:1708.04748 (2017)
https://bitcoin.nl/nieuws/bitcoin-privacy-173.

Legislation EU

3/2017: Amendment proposal on directive (EU) 2015/849

"Member States shall ensure that providers of exchanging services between virtual currencies and fiat currencies, custodian wallet providers, currency exchange and cheque cashing offices, and trust or company service providers are **licensed or registered**"

Maart 2017: European Parliament proposes amendment :
*"The Commission therefore proposes to make virtual currency exchange platforms and custodian wallet providers subject to some of the same **reporting obligations** as traditional financial service providers. In this framework, national FIUs (Financial Intelligence Units) **should be able to associate virtual currency addresses with***

Bitcoin is pseudonymous
Identification attacks possible
Exchange platforms will identify you

Smals
ICT for society

7 Bitcoin is trustless

We trust…

Bitcoin ≠ trustless

1. The correctness of the assumptions
2. The unhackability of out blockchain client
3. The unhackability of websites & trade platforms
4. Our infallibility (onfeilbaarheid)
5. Miners not to rewrite the blockchain collectively
6. That the value of Bitcoin will not collapse
7. That rules will not be changed against our interests
8. That the transaction fees will be acceptable

7 Bitcoin Myths

1. Bitcoin is money
2. Bitcoin is efficient
3. Bitcoin has perfect security
4. Bitcoin is a scarce asset, like gold
5. Bitcoin has low transaction costs
6. Bitcoin is anonymous
7. Bitcoin is trustless

Conclusion

Bitcoin is a 1st experiment with blockchain
We cannot expect that a 1st experiment is perfect
Hijacked by speculators

Future evolutions

- Legislation
- Technology (e.g. lightning network)

Questions & Contact

Dr. Kristof Verslype

Researcher, advisor & speaker
in crypto, privacy & blockchain tech

Smals Research
www.smalsresearch.be
@SmalsResearch

Smals ICT for society
www.smals.be
@Smals_ICT

Personal

www.cryptov.net
kristof.verslype@smals.be
@KristofVerslype
be.linkedin.com/in/verslype