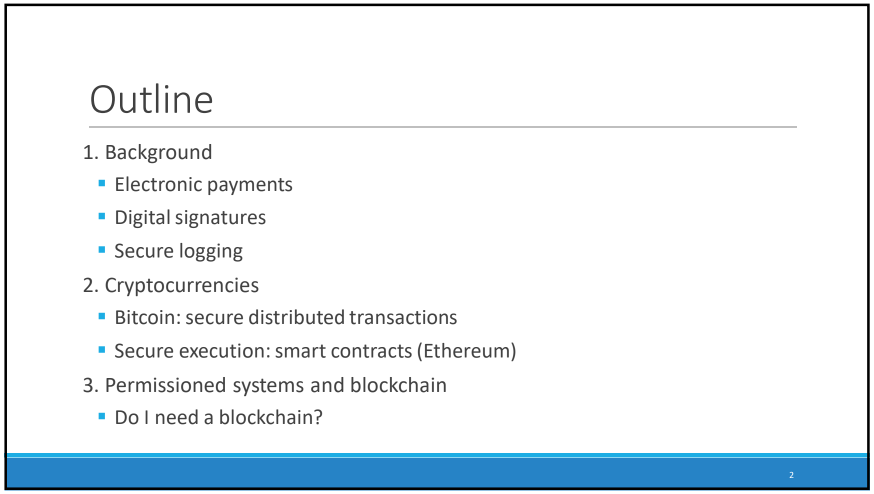
Cryptocurrencies and blockchains

PROF. DR. IR. BART PRENEEL COSIC KU LEUVEN, BELGIUM AND IMEC

FIRSTNAME.LASTNAME@ESAT.KULEUVEN.BE @BPRENEEL1

13 JUNE 2022

KU LEUVEN
imec
embracing a better life



Outline

1. Background
   - Electronic payments
   - Digital signatures
   - Secure logging
2. Cryptocurrencies
   - Bitcoin: secure distributed transactions
   - Secure execution: smart contracts (Ethereum)
3. Permissioned systems and blockchain
   - Do I need a blockchain?

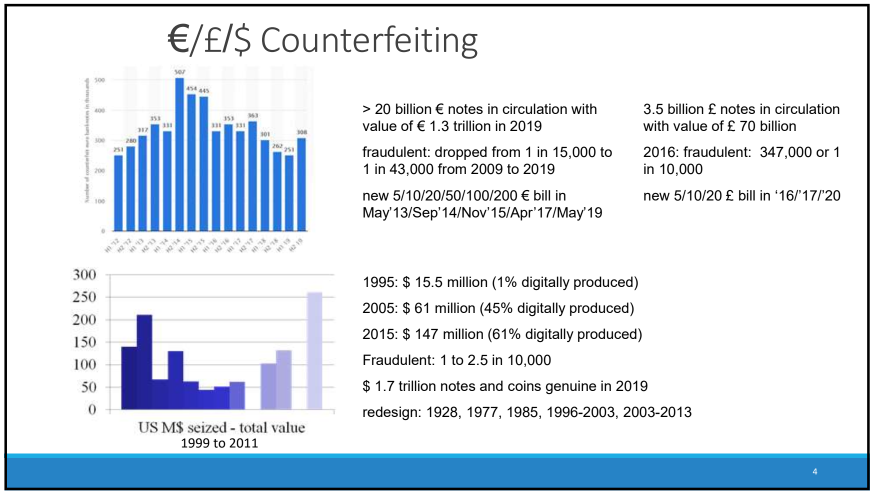
Currencies = maintaining memory

Susa, Iran, ca **3300 BC**

Cuneiform, Sumeria, ca **2600 BC**

David Graeber

Slide inspired by George Danezis



€/£/$ Counterfeiting

> 20 billion € notes in circulation with value of € 1.3 trillion in 2019

fraudulent: dropped from 1 in 15,000 to 1 in 43,000 from 2009 to 2019

new 5/10/20/50/100/200 € bill in May’13/Sep’14/Nov’15/Apr’17/May’19

3.5 billion £ notes in circulation with value of £ 70 billion

2016: fraudulent: 347,000 or 1 in 10,000

new 5/10/20 £ bill in ‘16/’17/’20

1999 to 2011

1995: $ 15.5 million (1% digitally produced)

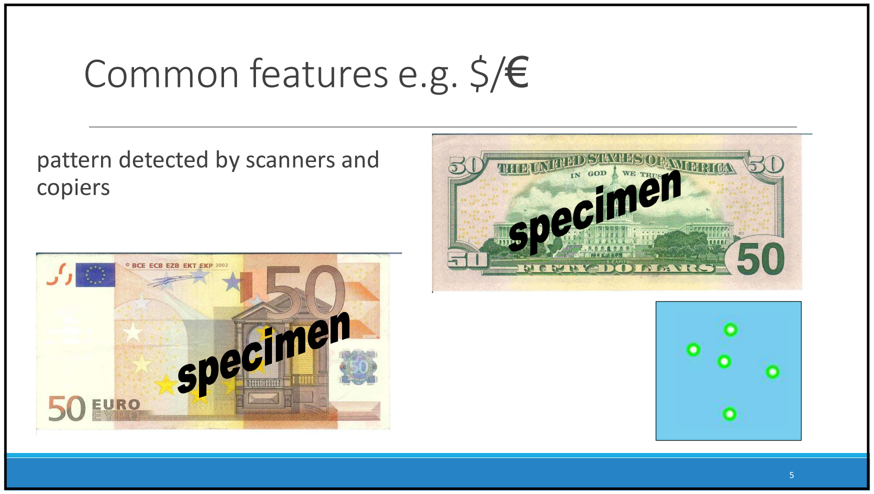
2005: $ 61 million (45% digitally produced)

2015: $ 147 million (61% digitally produced)

Fraudulent: 1 to 2.5 in 10,000

$ 1.7 trillion notes and coins genuine in 2019

redesign: 1928, 1977, 1985, 1996-2003, 2003-2013

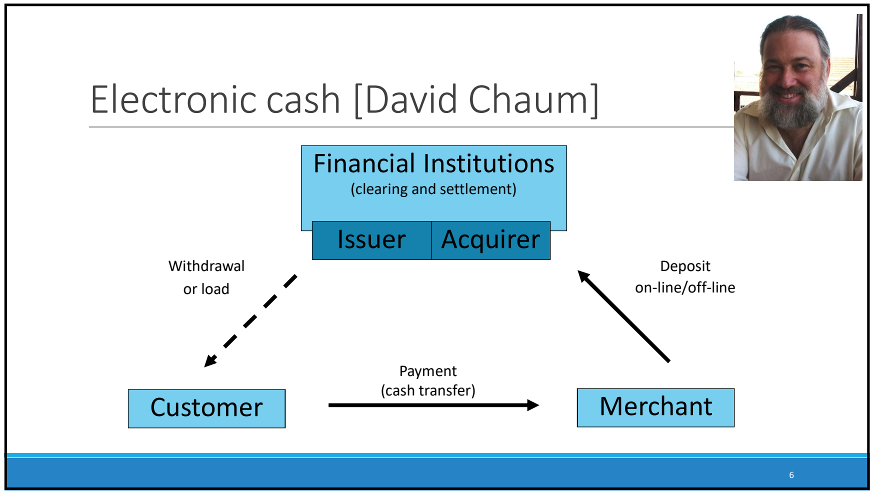


Common features e.g. $/€

pattern detected by scanners and copiers

specimen
50 EURO
specimen
THE UNITED STATES OF AMERICA
FIFTY DOLLARS
50

5



Electronic cash [David Chaum]

Financial Institutions
(clearing and settlement)

Issuer | Acquirer

Withdrawal
or load

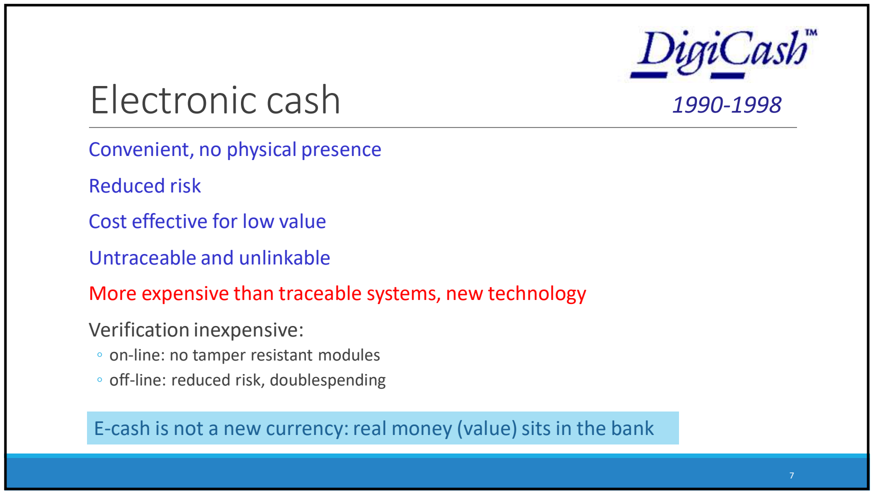
Deposit
on-line/off-line

Payment
(cash transfer)

Customer

Merchant

6



DigiCash™

1990-1998

Electronic cash

Convenient, no physical presence

Reduced risk

Cost effective for low value

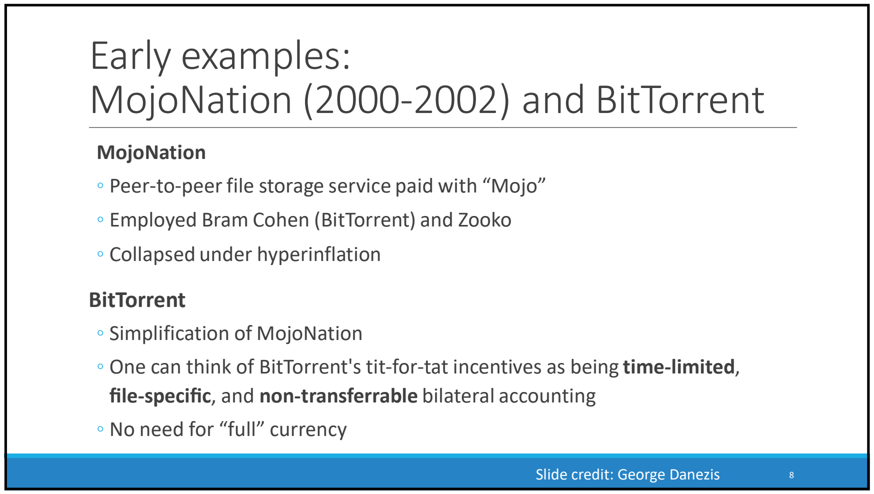
Untraceable and unlinkable

More expensive than traceable systems, new technology

Verification inexpensive:
- on-line: no tamper resistant modules
- off-line: reduced risk, doublespending

E-cash is not a new currency: real money (value) sits in the bank

7



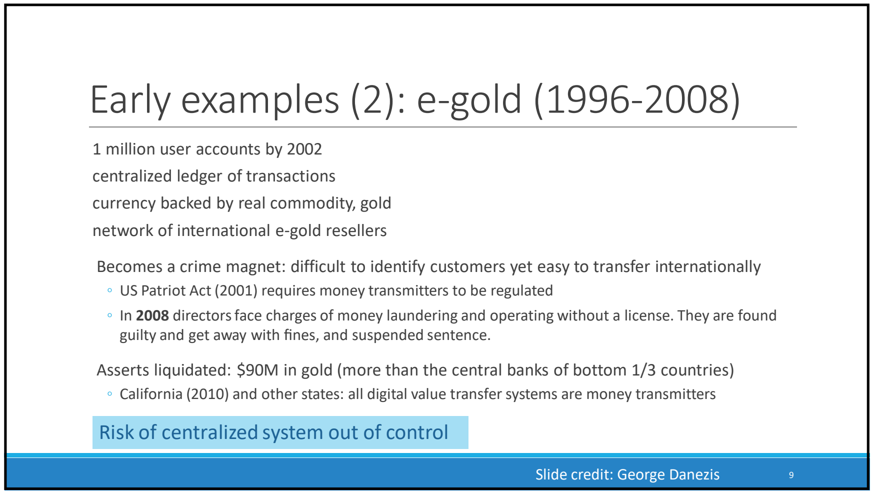
Early examples: MojoNation (2000-2002) and BitTorrent

MojoNation
- Peer-to-peer file storage service paid with “Mojo”
- Employed Bram Cohen (BitTorrent) and Zooko
- Collapsed under hyperinflation

BitTorrent
- Simplification of MojoNation
- One can think of BitTorrent's tit-for-tat incentives as being **time-limited**, **file-specific**, and **non-transferrable** bilateral accounting
- No need for “full” currency

Slide credit: George Danezis

8



Early examples (2): e-gold (1996-2008)

1 million user accounts by 2002

centralized ledger of transactions

currency backed by real commodity, gold

network of international e-gold resellers

Becomes a crime magnet: difficult to identify customers yet easy to transfer internationally

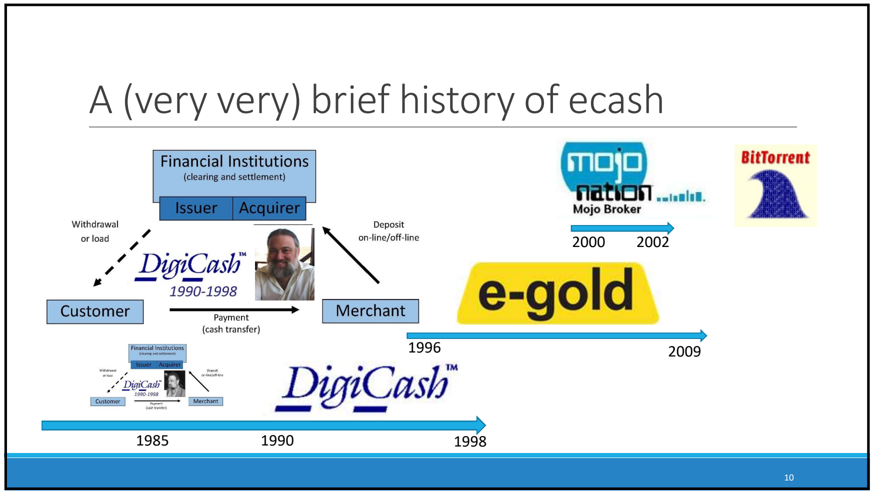
- US Patriot Act (2001) requires money transmitters to be regulated
- In **2008** directors face charges of money laundering and operating without a license. They are found guilty and get away with fines, and suspended sentence.

Asserts liquidated: $90M in gold (more than the central banks of bottom 1/3 countries)

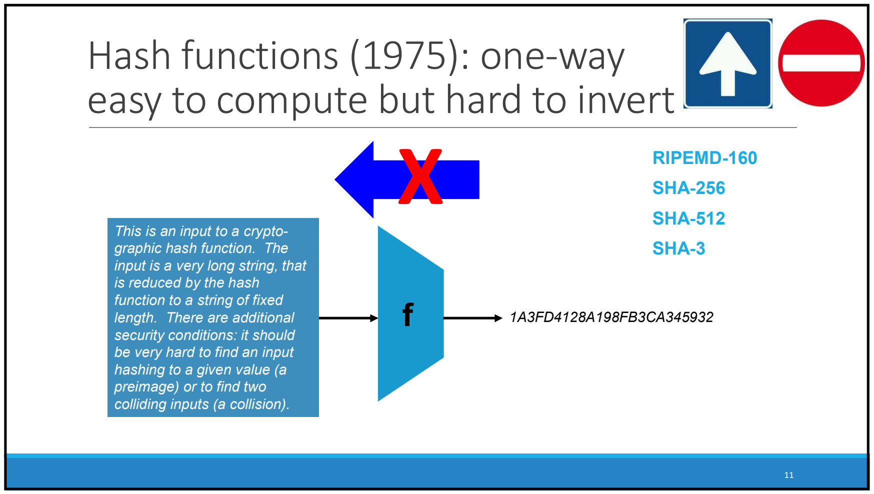
- California (2010) and other states: all digital value transfer systems are money transmitters

Risk of centralized system out of control

Slide credit: George Danezis

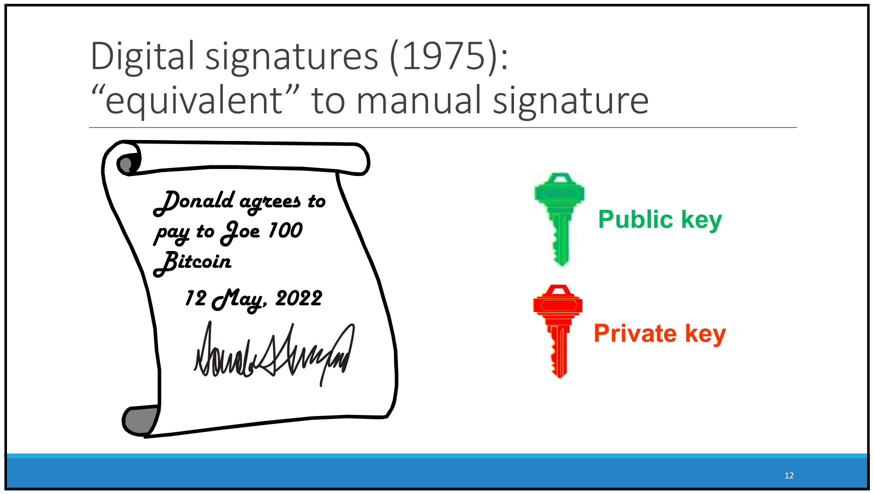


A (very very) brief history of ecash



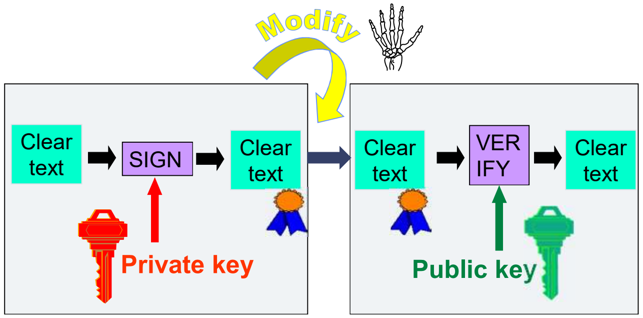
Hash functions (1975): one-way easy to compute but hard to invert

This is an input to a cryptographic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs (a collision).



Digital signatures (1975): “equivalent” to manual signature

Public key cryptology: digital signature



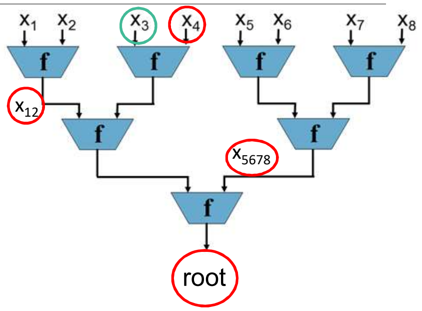
Merkle tree (1979)

Using a hash function f to authenticate a set of messages through a logarithmic number of values

Can check 2^n leaves of tree with a path of length $n = \log_2(2^n)$

This slide has example with n = 3: x_3 can be verified with x_4, x_{12}, x_{5678} and root

Applications: digital signatures, revocation…

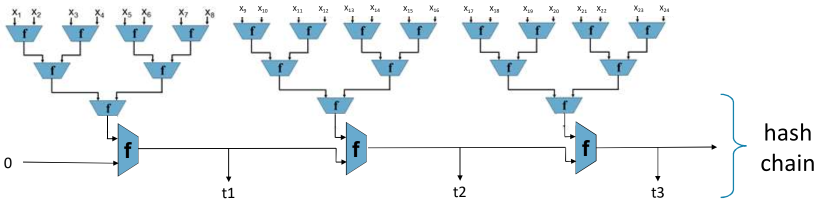


Timestamping (1990)

Collect documents and hash them with a Merkle tree

Chain these trees together with a hash chain

Publish intermediate values on a regular basis


x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8
x_9 x_{10} x_{11} x_{12} x_{13} x_{14} x_{15} x_{16}
x_{17} x_{18} x_{19} x_{20} x_{21} x_{22} x_{23} x_{24}
f
0
t1
t2
t3
hash chain

Timestamping: Surety Technologies (°1994)

http://www.surety.com/

AbsoluteProof® from Surety®
The Leader in Data Integrity Protection

Think of us as the 'Digital Wax Seal'

Intellectual Property Protection
Protect your patents, copy-rights, trademarks, and trade secrets »

Digital Evidence Protection
Preserve the integrity of your electronic evidence »

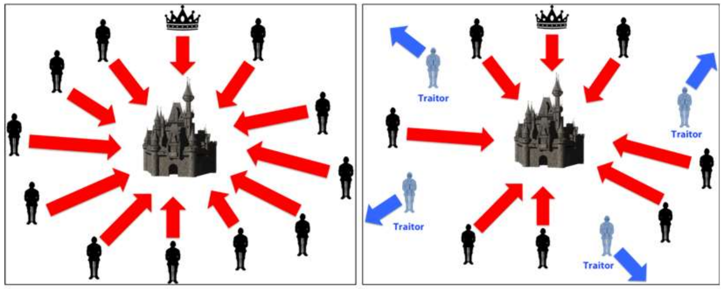
Electronic Record Authenticity
Defend the authenticity of your electronic records »

Protect the Integrity, Defend the Authenticity of Your Digital Information

https://www.belspo.be/belspo/organisation/Publ/pub_ostc/NO/rNOb007_en.pdf
Belgian TIMESEC project (1996-1998)

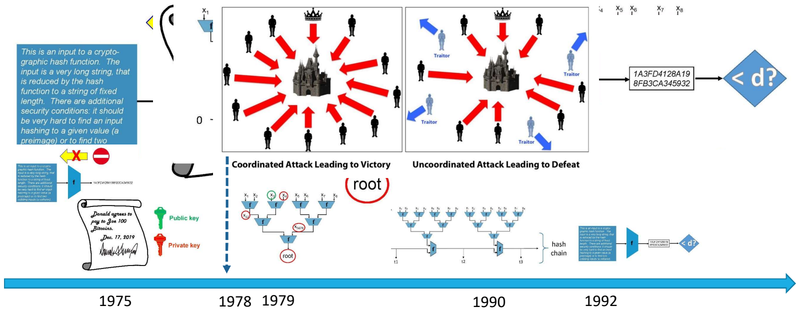
Estonia: Cybernetica

Byzantine generals problem
(can deal with at most 1/3 traitors)



Coordinated Attack Leading to Victory **Uncoordinated Attack Leading to Defeat**

Technologies underlying Bitcoin



This is an input to a cryptographic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two

Donald agrees to pay to Joe 100 Bitcoins. Dec. 17, 2019
Public key
Private key
Coordinated Attack Leading to Victory
Uncoordinated Attack Leading to Defeat
Traitor
root
f
1A3FD4128A19 8FB3CA345932
< d?
hash chain
1975
1978
1979
1990
1992

Part 2 Cryptocurrencies

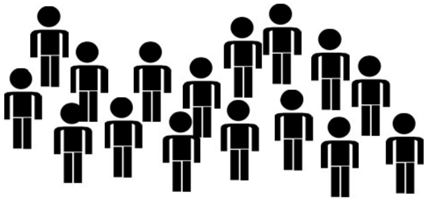
1. Background
   - Electronic payments
   - Digital signatures
   - Secure logging
2. Cryptocurrencies
   - Bitcoin: secure distributed transactions
   - Secure execution: smart contracts (Ethereum)
3. Permissioned systems and blockchain
   - Do I need a blockchain?

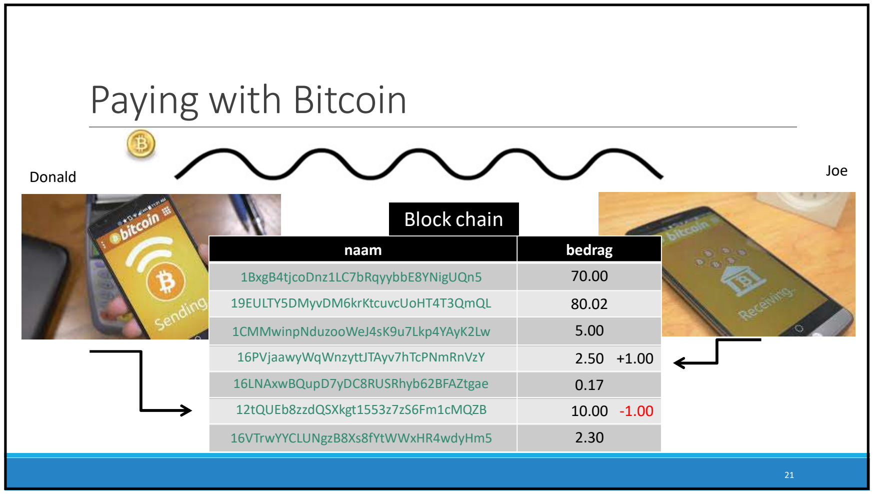
Bitcoin (2008): Satoshi Nakamoto

No central bank

Everyone can produce money

Everyone can verify transactions





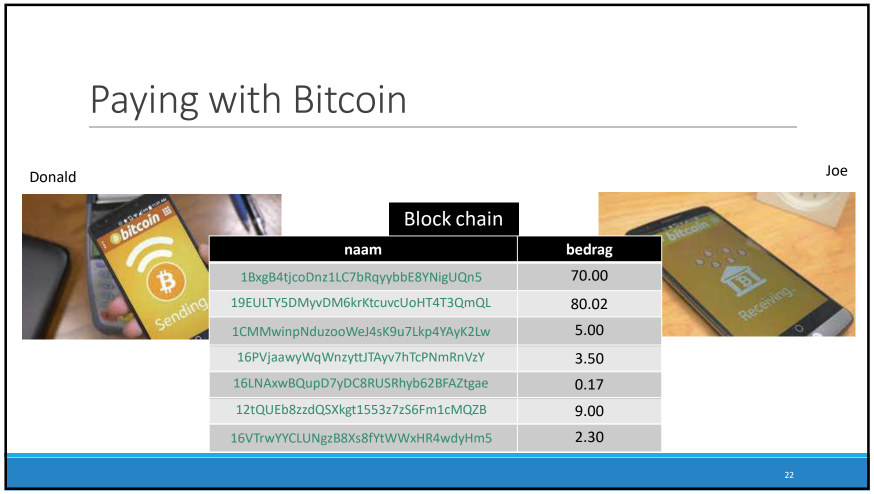
Paying with Bitcoin

Donald

Joe

Block chain

naam	bedrag
1BxgB4tjcoDnz1LC7bRqyybbE8YNigUQn5	70.00
19EULTY5DMyvDM6krKtcuvcUoHT4T3QmQL	80.02
1CMMwinpNduzooWeJ4sK9u7Lkp4YAyK2Lw	5.00
16PVjaawyWqWnzyttJTAyv7hTcPNmRnVzY	2.50 +1.00
16LNAxwBQupD7yDC8RUSRhyb62BFAZtgae	0.17
12tQUEb8zzdQSXkgt1553z7zS6Fm1cMQZB	10.00 -1.00
16VTrwYYCLUNgzB8Xs8fYtWWxHR4wdyHm5	2.30



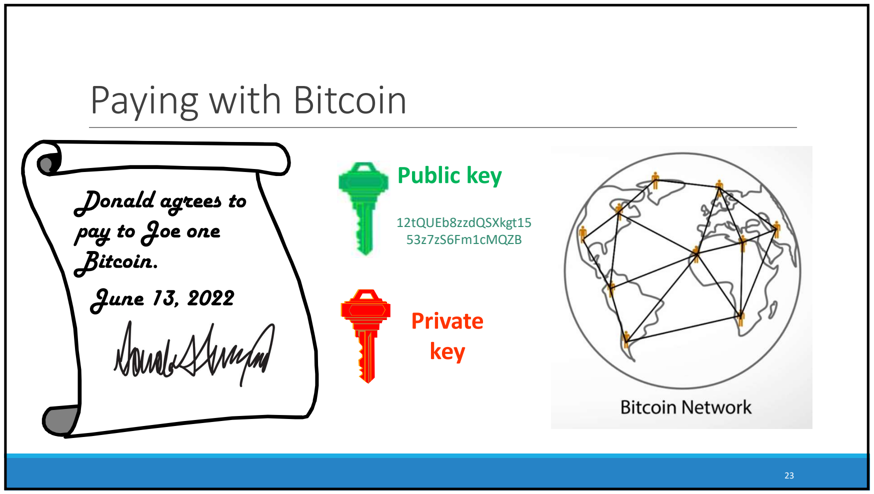
Paying with Bitcoin

Donald

Joe

Block chain

naam	bedrag
1BxgB4tjcoDnz1LC7bRqyybbE8YNigUQn5	70.00
19EULTY5DMyvDM6krKtcuvcUoHT4T3QmQL	80.02
1CMMwinpNduzooWeJ4sK9u7Lkp4YAyK2Lw	5.00
16PVjaawyWqWnzyttJTAyv7hTcPNmRnVzY	3.50
16LNAxwBQupD7yDC8RUSRhyb62BFAZtgae	0.17
12tQUEb8zzdQSXkgt1553z7zS6Fm1cMQZB	9.00
16VTrwYYCLUNgzB8Xs8fYtWWxHR4wdyHm5	2.30



Paying with Bitcoin

Donald agrees to pay to Joe one Bitcoin.

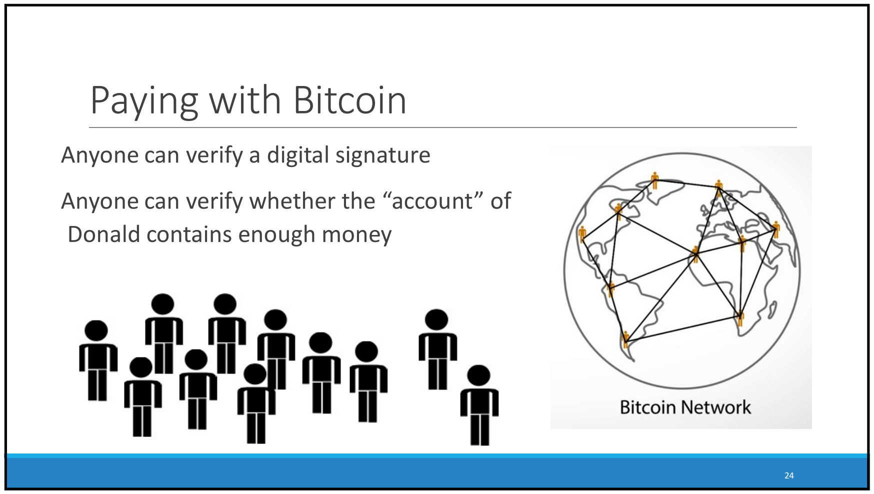
June 13, 2022

Public key

12tQUEb8zzdQSXkgt15
53z7zS6Fm1cMQZB

Private key

Bitcoin Network



Paying with Bitcoin

Anyone can verify a digital signature

Anyone can verify whether the "account" of Donald contains enough money

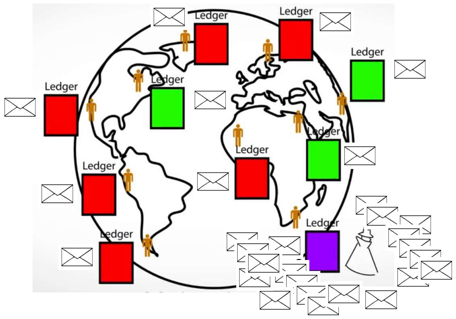
Bitcoin Network

Managing the blockchain

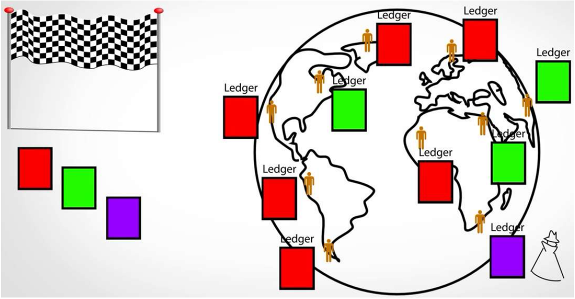
Miners all over the world follow up all the transactions

But due to communication errors or fraud there are multiple versions

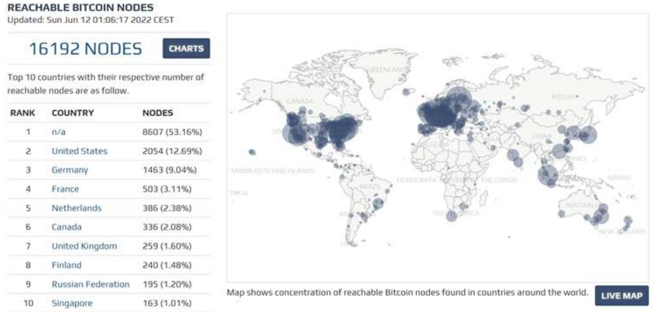
Voting?



Puzzles (a lottery)



The Bitcoin network



REACHABLE BITCOIN NODES
Updated: Sun Jun 12 01:06:17 2022 CEST

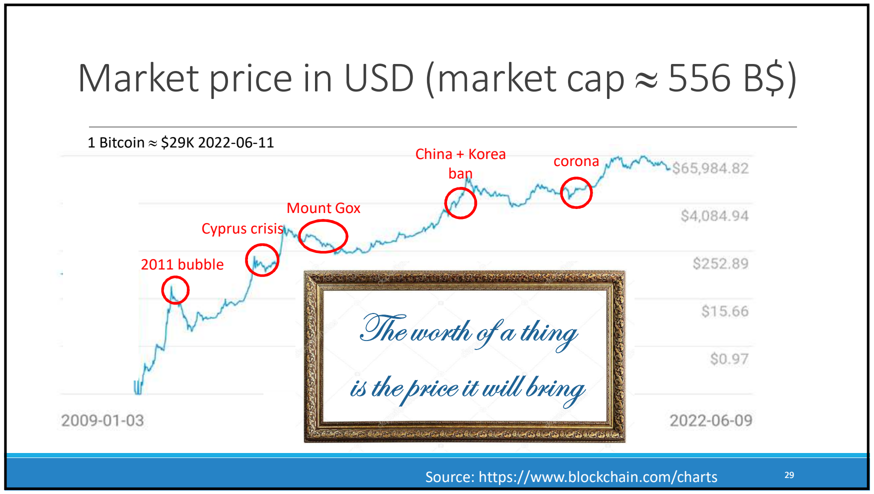
16192 NODES

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	8607 (53.16%)
2	United States	2054 (12.69%)
3	Germany	1463 (9.04%)
4	France	503 (3.11%)
5	Netherlands	386 (2.38%)
6	Canada	336 (2.08%)
7	United Kingdom	259 (1.60%)
8	Finland	240 (1.48%)
9	Russian Federation	195 (1.20%)
10	Singapore	163 (1.01%)

Map shows concentration of reachable Bitcoin nodes found in countries around the world.

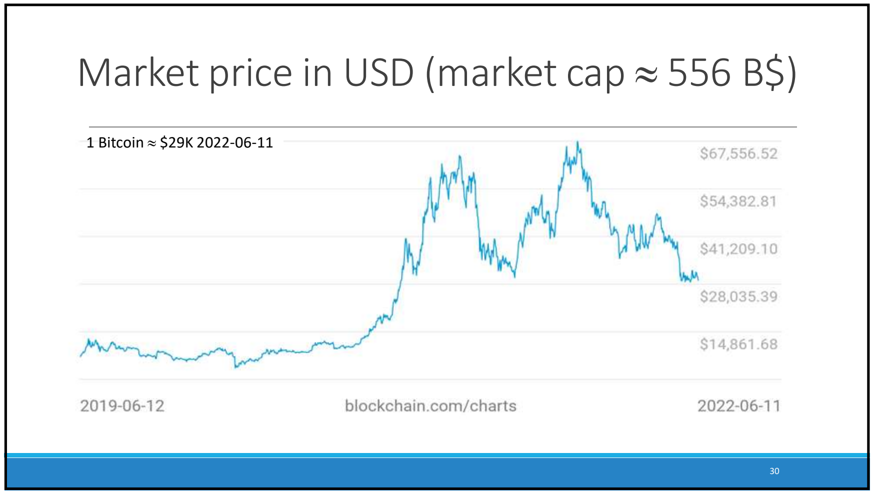
Source: https://bitnodes.io/



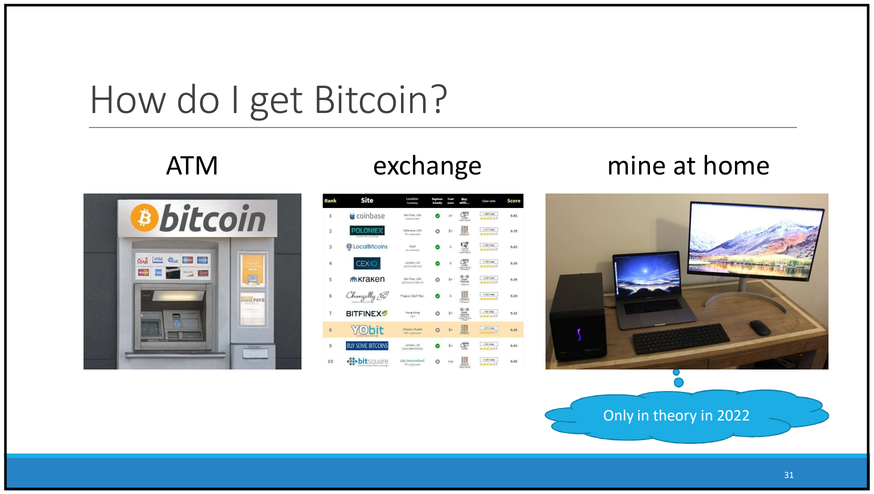
Market price in USD (market cap ≈ 556 B$)

The worth of a thing is the price it will bring

Source: https://www.blockchain.com/charts

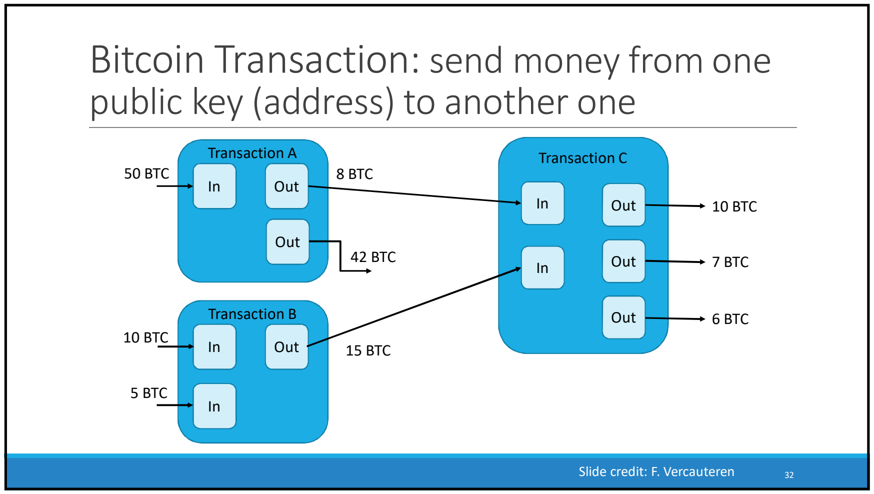


Market price in USD (market cap ≈ 556 B$)



How do I get Bitcoin?

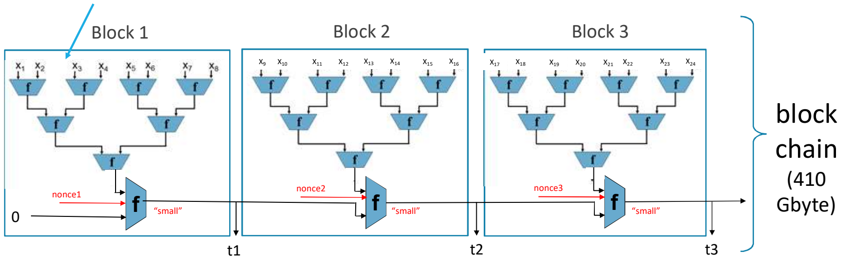
Only in theory in 2022



Bitcoin Transaction: send money from one public key (address) to another one

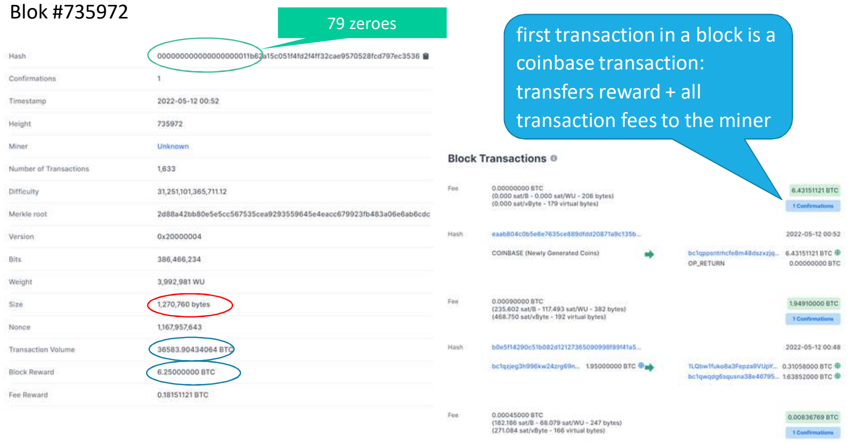
Slide credit: F. Vercauteren

Block Chain: a public decentralized ledger


Bitcoin transactions
Block 1
Block 2
Block 3
x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8
x_9 x_{10} x_{11} x_{12} x_{13} x_{14} x_{15} x_{16}
x_{17} x_{18} x_{19} x_{20} x_{21} x_{22} x_{23} x_{24}
f
nonce1
nonce2
nonce3
"small"
0
t1
t2
t3
block chain (410 Gbyte)

Also include in every block timestamp and difficulty level of puzzle

Blok #735972



79 zeroes

first transaction in a block is a coinbase transaction: transfers reward + all transaction fees to the miner

Hash	0000000000000000000011b62a15c051f4fd2f4ff32cae9570528fcd797ec3536
Confirmations	1
Timestamp	2022-05-12 00:52
Height	735972
Miner	Unknown
Number of Transactions	1,633
Difficulty	31,251,101,365,711.12
Merkle root	2d88a42bb80e5e5cc567535cea9293559645e4eacc679923fb483a06e6ab6cdc
Version	0x20000004
Bits	386,466,234
Weight	3,992,981 WU
Size	1,270,760 bytes
Nonce	1,167,957,643
Transaction Volume	36583.90434064 BTC
Block Reward	6.25000000 BTC
Fee Reward	0.18151121 BTC

Block Transactions

Fee 0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 206 bytes)
(0.000 sat/vByte - 179 virtual bytes)
6.43151121 BTC
1 Confirmations

Hash eaab804c0b5e6e7635ce889dfdd20871a9c135b... 2022-05-12 00:52
COINBASE (Newly Generated Coins) → bc1qppsntrhcfe8m48dszxzjq... 6.43151121 BTC
OP_RETURN 0.00000000 BTC

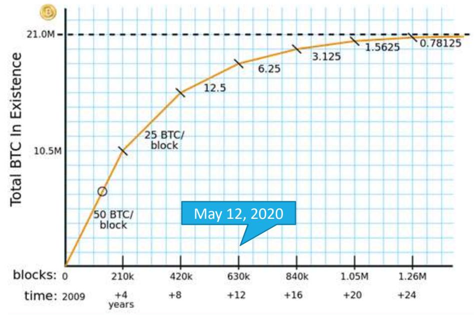
Fee 0.00090000 BTC
(235.602 sat/B - 117.493 sat/WU - 382 bytes)
(468.750 sat/vByte - 192 virtual bytes)
1.94910000 BTC
1 Confirmations

Hash b0e5f14290c51b082d1212736509099 8f89f41a5... 2022-05-12 00:48
bc1qzjeg3h996kw24zrg69n... 1.95000000 BTC → 1LQbw1fuko8a3Fepza9VUpY... 0.31058000 BTC
bc1qwqdg6squsna38e46795... 1.63852000 BTC

Fee 0.00045000 BTC
(182.186 sat/B - 68.079 sat/WU - 247 bytes)
(271.084 sat/vByte - 166 virtual bytes)
0.00836769 BTC
1 Confirmations

https://www.blockchain.com/btc/block/0000000000000000000011b62a15c051f4fd2f4ff32cae9570528fcd797ec3536

Mining rewards

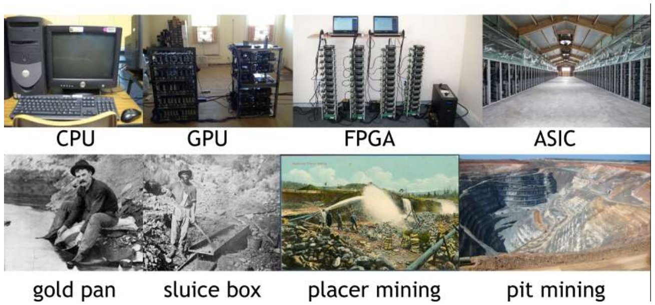


Total number of Bitcoins is limited to 21 million, each divided in 8 decimal places leading to 21×10^{14} units

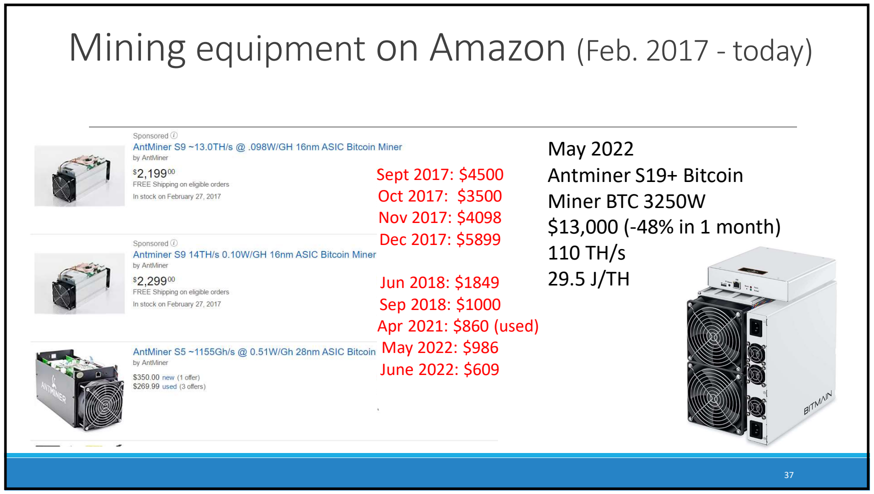
May 2022: 19.03 million BTC mined, 91% of total

Figure by Chris Pacia

Mining has become industrial



Slide credit: Joseph Bonneau



Mining equipment on Amazon (Feb. 2017 - today)

Sponsored
AntMiner S9 ~13.0TH/s @ .098W/GH 16nm ASIC Bitcoin Miner
by AntMiner
$\$2{,}199^{00}$
FREE Shipping on eligible orders
In stock on February 27, 2017

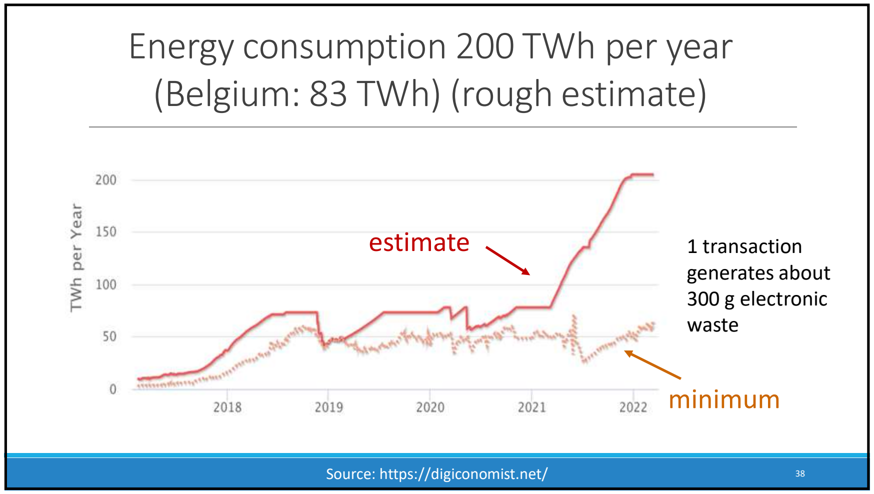
Sponsored
Antminer S9 14TH/s 0.10W/GH 16nm ASIC Bitcoin Miner
by AntMiner
$\$2{,}299^{00}$
FREE Shipping on eligible orders
In stock on February 27, 2017

AntMiner S5 ~1155Gh/s @ 0.51W/Gh 28nm ASIC Bitcoin
by AntMiner
$350.00 new (1 offer)
$269.99 used (3 offers)

Sept 2017: $4500
Oct 2017: $3500
Nov 2017: $4098
Dec 2017: $5899

Jun 2018: $1849
Sep 2018: $1000
Apr 2021: $860 (used)
May 2022: $986
June 2022: $609

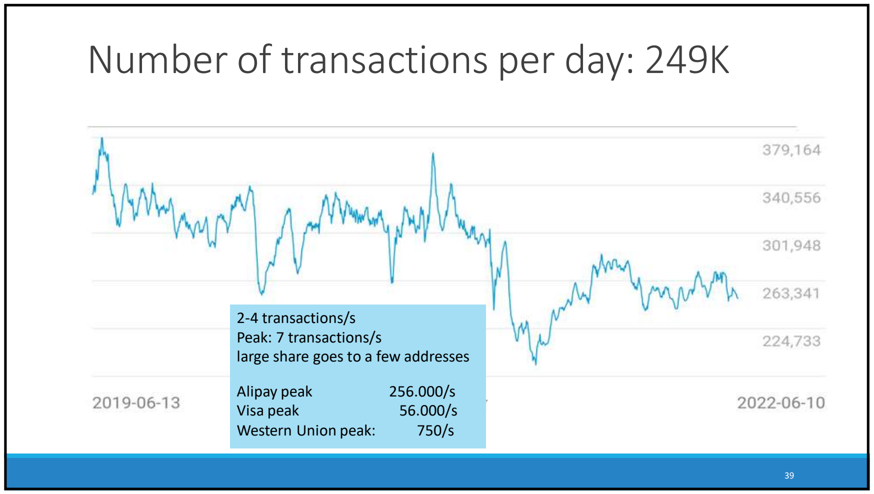
May 2022
Antminer S19+ Bitcoin
Miner BTC 3250W
$13,000 (-48% in 1 month)
110 TH/s
29.5 J/TH



Energy consumption 200 TWh per year (Belgium: 83 TWh) (rough estimate)

1 transaction generates about 300 g electronic waste

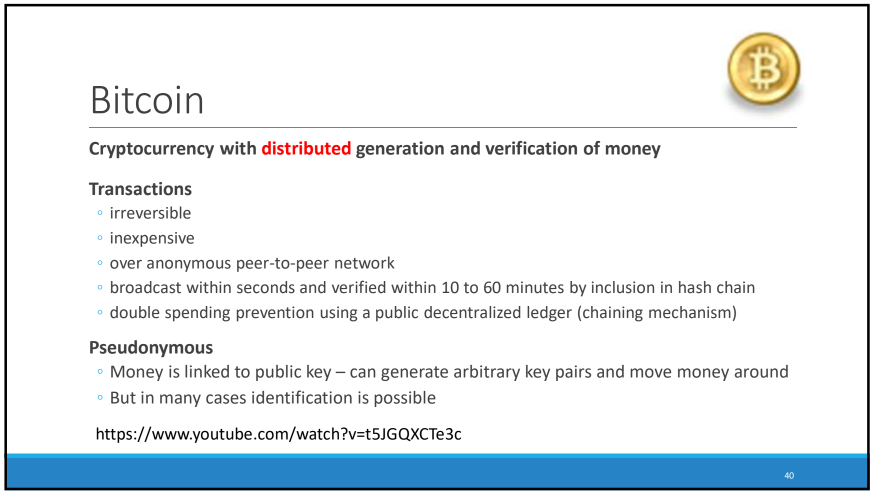
Source: https://digiconomist.net/



Number of transactions per day: 249K

2-4 transactions/s
Peak: 7 transactions/s
large share goes to a few addresses

Alipay peak	256.000/s
Visa peak	56.000/s
Western Union peak:	750/s



Bitcoin

Cryptocurrency with distributed generation and verification of money

Transactions
- irreversible
- inexpensive
- over anonymous peer-to-peer network
- broadcast within seconds and verified within 10 to 60 minutes by inclusion in hash chain
- double spending prevention using a public decentralized ledger (chaining mechanism)

Pseudonymous
- Money is linked to public key – can generate arbitrary key pairs and move money around
- But in many cases identification is possible

https://www.youtube.com/watch?v=t5JGQXCTe3c

Bitcoin as a currency

Who has control of the money supply in a currency?

- By convention it follows a well understood and committed curve that will max out
- Convention enforced by software

Who gets the new money? Who deletes the old money?

- No money is deleted (if you want a laugh: go suggest random deletions!)
- Money is created by hashing blocks and adding them to the block chain
- The miner gets the new coin

How do we make sure we will always remember who has how much money?

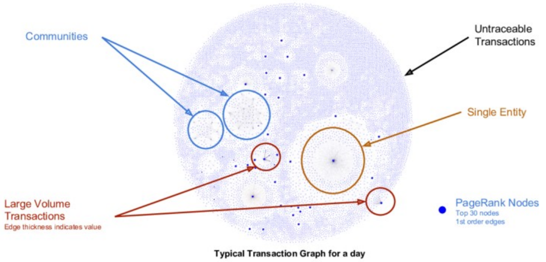
- Large block--chain is recorded by all (April 2021 341 GByte)
- Authoritative one is the longest – race for aggregate CPU power

Who has it to start with? (Does it matter?)

- Satoshi Nakamoto

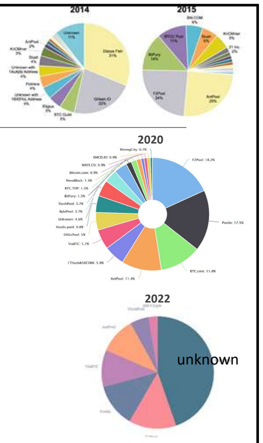
Slide credit: George Danezis

Does Bitcoin offer privacy?



Typical Transaction Graph for a day

Some observations on Bitcoin



Cryptocurrency community aspires to be mainstream but behaves as rebels

- this is not sustainable

Volatile

Paying and secure storage somewhat complex

No peace of mind for users: if you are hacked, tough luck
All miners are concentrated

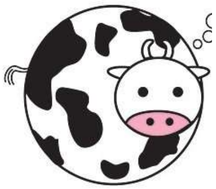
Incentives system complex

Ideas have definitely made a major impact

Open issues

Resistance to attacks

- Sybil attack: attacker controls many nodes in network, can refuse relaying or favouring his own blocks
- Selfish mining attack
- Bribery



Is Bitcoin incentive compatible?

- Convergence
- Fairness
- Liveliness

Some proof exist in simplified models

Ethereum (ETH)

https://www.ethereum.org/ https://etherscan.io/

White paper 2013, live July 2015

Smart contract (scripting) functionality: deterministic exchange mechanisms controlled by digital means that can carry out the direct transaction of value between untrusted agents

- E.g. self-contained fair casinos, currency swap, automated insurance for air travel

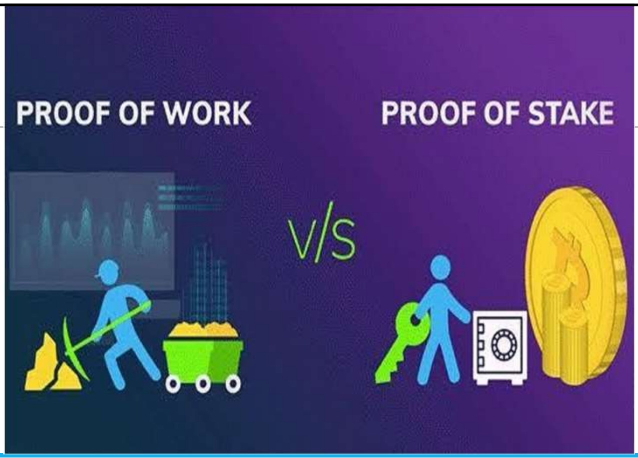
Large decentralized computer where everyone can verify the outcome of computations

Need to make reliable connection with physical world

Currency is called “ether” – internal transaction pricing with “gas” (anti-DDOS and spam)

Ethereum forks

- 2016: DAO hack led to ETC fork (Ethereum classic)
- Q4/2016: 2 additional forks



Proof of stake

First suggested in an online forum in 2011

Miners stake coins

Miners solve “easy”puzzles based on information of the stakes, round number and public randomness

More scalable than PoW

Validators need to be online

Peercoin (PPC) (‘12): hybrid PoS/PoW

NXT (‘14)

Tezos (XTZ) (‘14)

BlackCoin (BLK) (‘14)

Ethereum 2.0 (ETH): Casper FFG (‘15)

Polkadot (DOT) (‘16)

Cardano (ADA): Ourobouros (‘17)

Solana (SOL) (‘19)

Proof of stake: foundations

Miners solve “easy” puzzles based on information of the stakes, round number and public randomness

Cryptographic idea: verifiable random functions (VRF)

Schemes with rigorous analysis

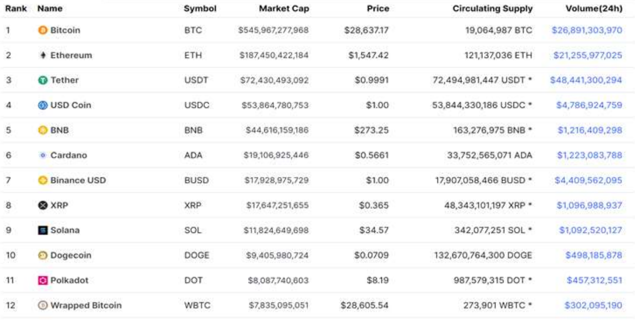
- Bitcoin-style: Sleepy (‘17), Ouroboros Praos (‘17-‘18), Ouroboros Genesis (‘18), Snow White (‘19), Bagaria et al. (‘19)
- Multiple rounds of communications: Algorand (‘17), Ouroboros (‘16), EOS (‘18), Dfinity (‘18)
- Block-by-block protocol (rather than epochs): Fan-Katz-Thai-Zhou (‘17-’21)

Cryptocurrencies:
Total market cap $1246 B

Total value of all gold?
Total value of stock exchange?

12 T$
110 T$

PoW
PoW -> PoS
---
multichain
BFT
PoS
stablecoin
BFT
PoS
PoW
PoS
ERC20/BTC



Rank	Name	Symbol	Market Cap	Price	Circulating Supply	Volume(24h)
1	Bitcoin	BTC	$545,967,277,968	$28,637.17	19,064,987 BTC	$26,891,303,970
2	Ethereum	ETH	$187,450,422,184	$1,547.42	121,137,036 ETH	$21,255,977,025
3	Tether	USDT	$72,430,493,092	$0.9991	72,494,981,447 USDT *	$48,441,300,294
4	USD Coin	USDC	$53,864,780,753	$1.00	53,844,330,186 USDC *	$4,786,924,759
5	BNB	BNB	$44,616,159,186	$273.25	163,276,975 BNB *	$1,216,409,298
6	Cardano	ADA	$19,106,925,446	$0.5661	33,752,565,071 ADA	$1,223,083,788
7	Binance USD	BUSD	$17,928,975,729	$1.00	17,907,058,466 BUSD *	$4,409,562,095
8	XRP	XRP	$17,647,251,655	$0.365	48,343,101,197 XRP *	$1,096,988,937
9	Solana	SOL	$11,824,649,698	$34.57	342,077,251 SOL *	$1,092,520,127
10	Dogecoin	DOGE	$9,405,980,724	$0.0709	132,670,764,300 DOGE	$498,185,878
11	Polkadot	DOT	$8,087,740,603	$8.19	987,579,315 DOT *	$457,312,551
12	Wrapped Bitcoin	WBTC	$7,835,095,051	$28,605.54	273,901 WBTC *	$302,095,190

Source: https://coinmarketcap.com/all/views/all/

Proof of Work versus Proof of Stake?

Proof of stake: weaknesses and defenses

51% attack

Centralization

Attack on infrastructure

Long range: overtake chain starting from genesis block

Nothing-at-stake: validator vouches for multiple chains

It is not so easy to acquire a large share of currency/mining power

Attack will result in price drop

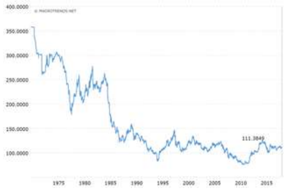
Better alignment between different players than in PoW

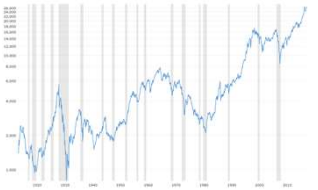
Making a profit with double spending requires large transaction volume

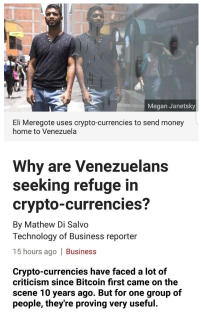
Is Bitcoin is the money of the future?

3 main purposes of money
- medium of exchange
- store of value
- unit of account

Computer scientists set the monetary policy
We don't understand Bitcoin







Megan Janetsky

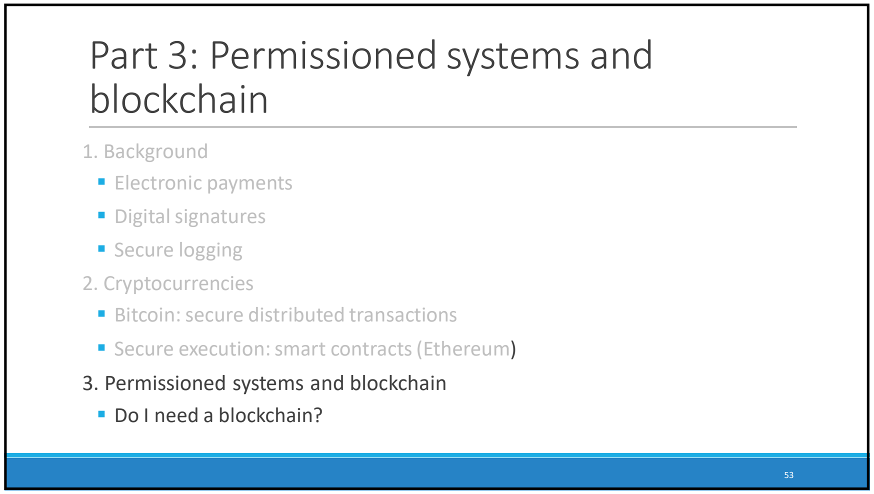
Eli Meregote uses crypto-currencies to send money home to Venezuela

Why are Venezuelans seeking refuge in crypto-currencies?

By Mathew Di Salvo
Technology of Business reporter

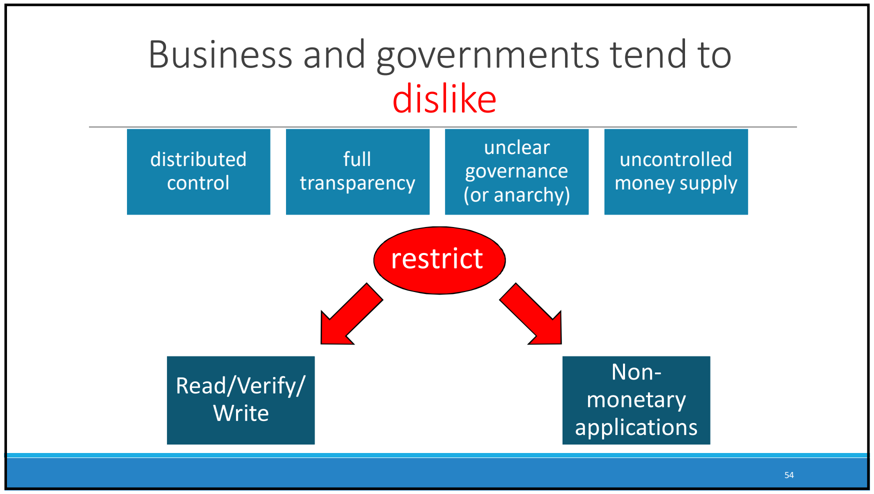
15 hours ago | Business

Crypto-currencies have faced a lot of criticism since Bitcoin first came on the scene 10 years ago. But for one group of people, they're proving very useful.



Part 3: Permissioned systems and blockchain

1. Background
   - Electronic payments
   - Digital signatures
   - Secure logging
2. Cryptocurrencies
   - Bitcoin: secure distributed transactions
   - Secure execution: smart contracts (Ethereum)
3. Permissioned systems and blockchain
   - Do I need a blockchain?



Business and governments tend to dislike

distributed control

full transparency

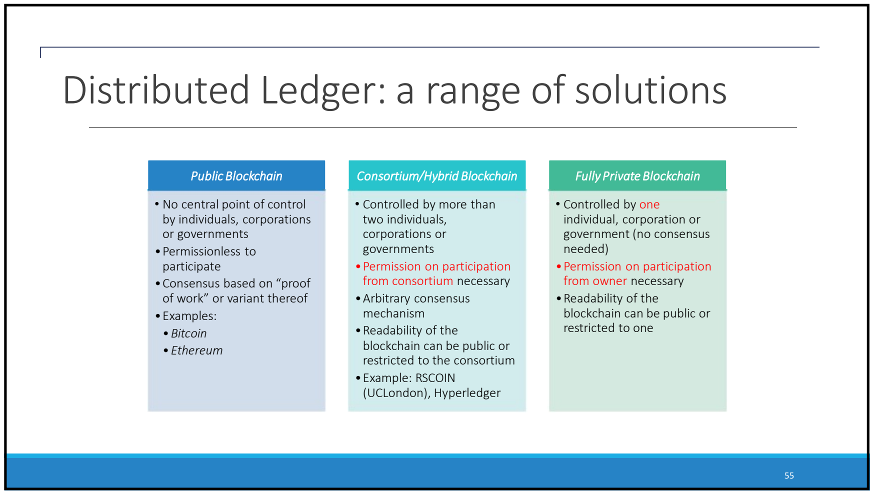
unclear governance (or anarchy)

uncontrolled money supply

restrict

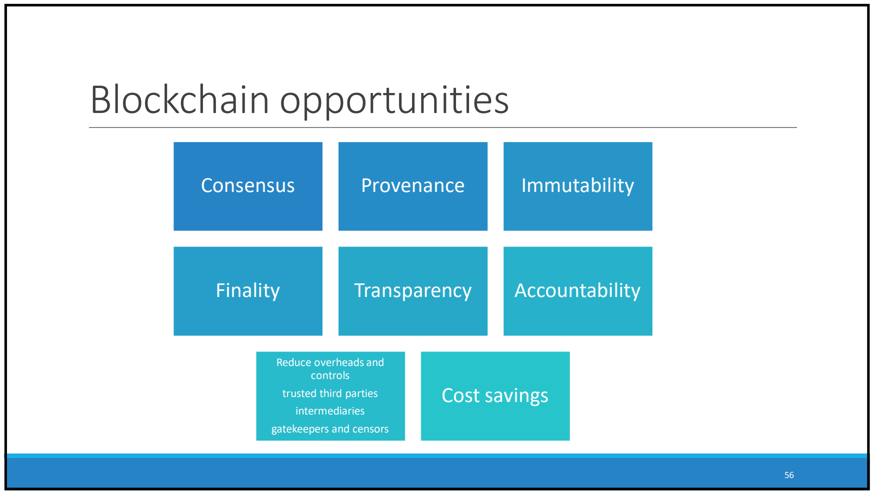
Read/Verify/ Write

Non-monetary applications



Distributed Ledger: a range of solutions

Public Blockchain	*Consortium/Hybrid Blockchain*	*Fully Private Blockchain*
• No central point of control by individuals, corporations or governments • Permissionless to participate • Consensus based on "proof of work" or variant thereof • Examples: • *Bitcoin* • *Ethereum*	• Controlled by more than two individuals, corporations or governments • Permission on participation from consortium necessary • Arbitrary consensus mechanism • Readability of the blockchain can be public or restricted to the consortium • Example: RSCOIN (UCLondon), Hyperledger	• Controlled by one individual, corporation or government (no consensus needed) • Permission on participation from owner necessary • Readability of the blockchain can be public or restricted to one



Blockchain opportunities

Consensus

Provenance

Immutability

Finality

Transparency

Accountability

Reduce overheads and controls

trusted third parties

intermediaries

gatekeepers and censors

Cost savings

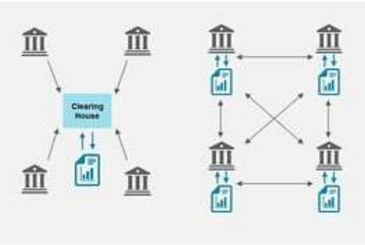
Shared replicated permissioned ledger

The Economist | Topics | Current edition | More | 2015

The promise of the blockchain

The trust machine

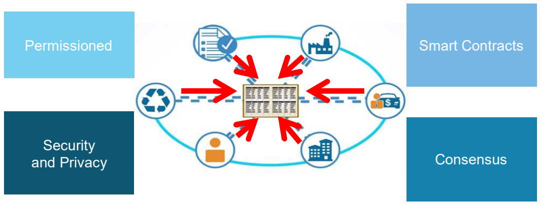
The technology behind bitcoin could transform how the economy works



All technical building blocks of distributed ledgers were developed by 1990

Figure https://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/

Shared ledger



Permissioned

Smart Contracts

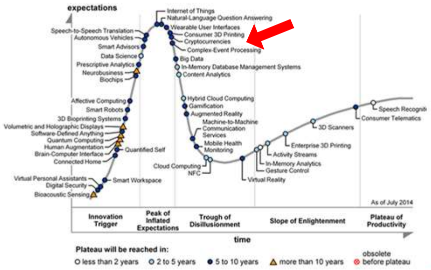
Security and Privacy

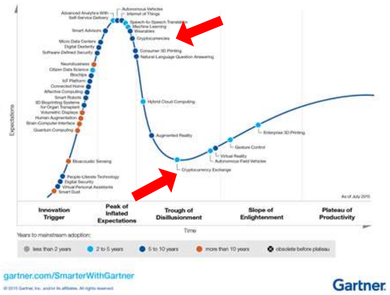
Consensus

Smart contracts: $315M in 2021 (CACG 24%)

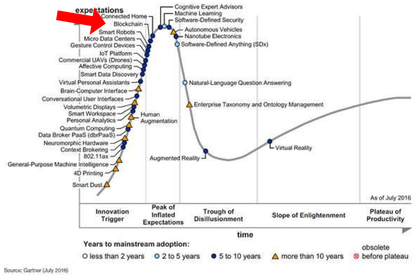
https://reports.valuates.com/market-reports/QYRE-Auto-31L1599/global-smart-contracts

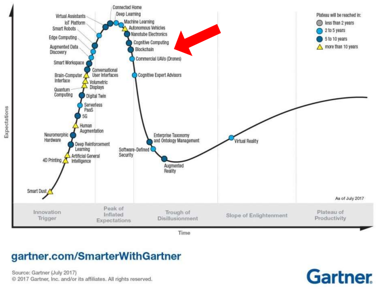
Gartner Hype Cycle Emerging Technologies Cryptocurrencies 2014-2015

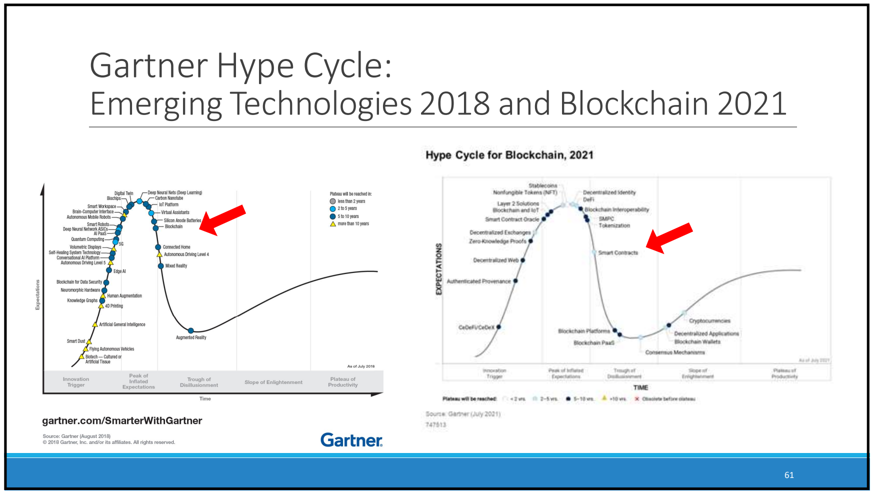




Gartner Hype Cycle Emerging Technologies Blockchain 2016-2017







Gartner Hype Cycle: Emerging Technologies 2018 and Blockchain 2021

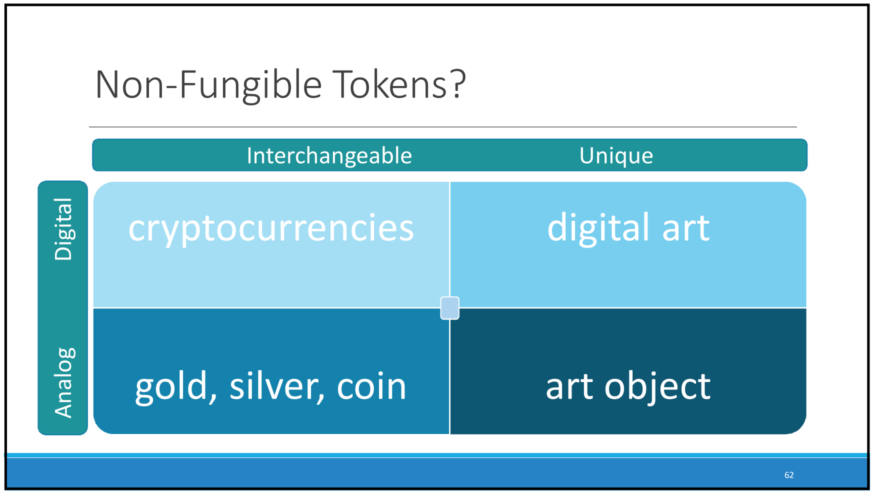
gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

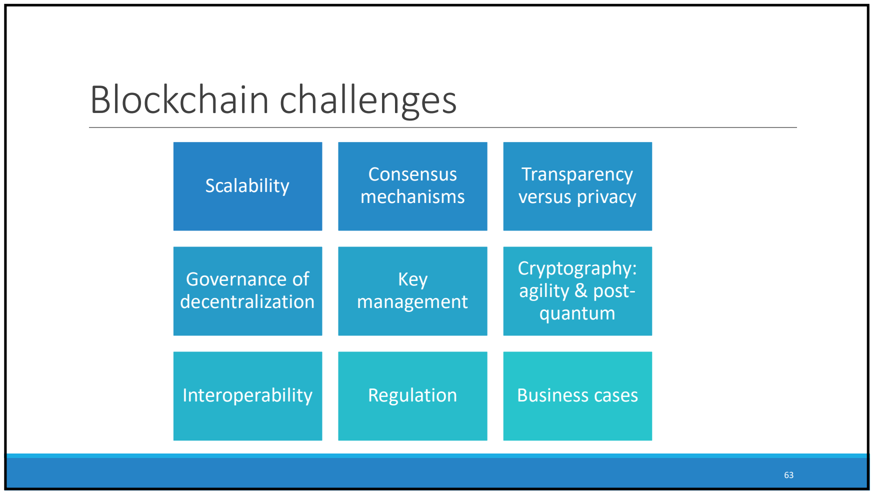
Hype Cycle for Blockchain, 2021

Source: Gartner (July 2021)
747513



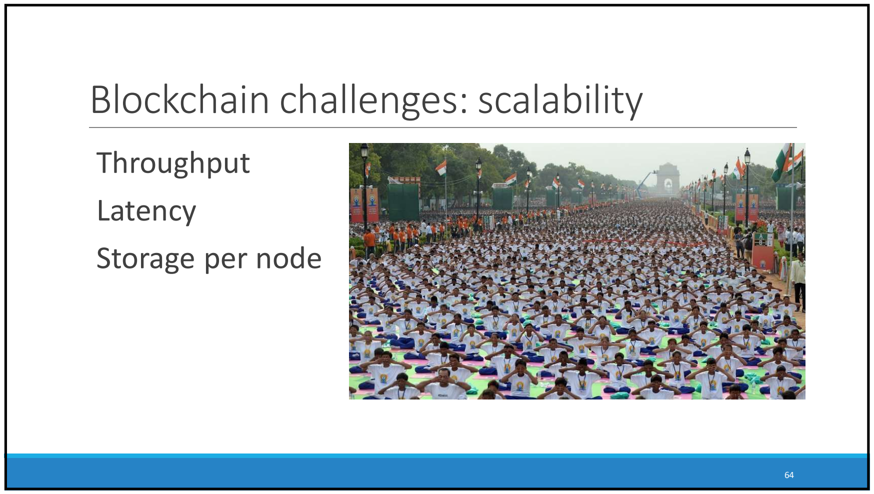
Non-Fungible Tokens?

	Interchangeable	Unique
Digital	cryptocurrencies	digital art
Analog	gold, silver, coin	art object



Blockchain challenges

Scalability	Consensus mechanisms	Transparency versus privacy
Governance of decentralization	Key management	Cryptography: agility & post-quantum
Interoperability	Regulation	Business cases

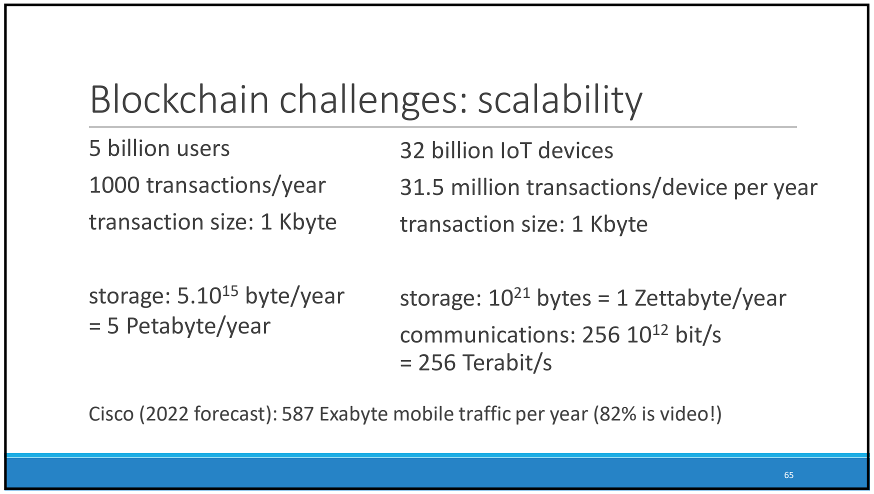


Blockchain challenges: scalability

Throughput

Latency

Storage per node



Blockchain challenges: scalability

5 billion users

1000 transactions/year

transaction size: 1 Kbyte

storage: 5.10^{15} byte/year
= 5 Petabyte/year

32 billion IoT devices

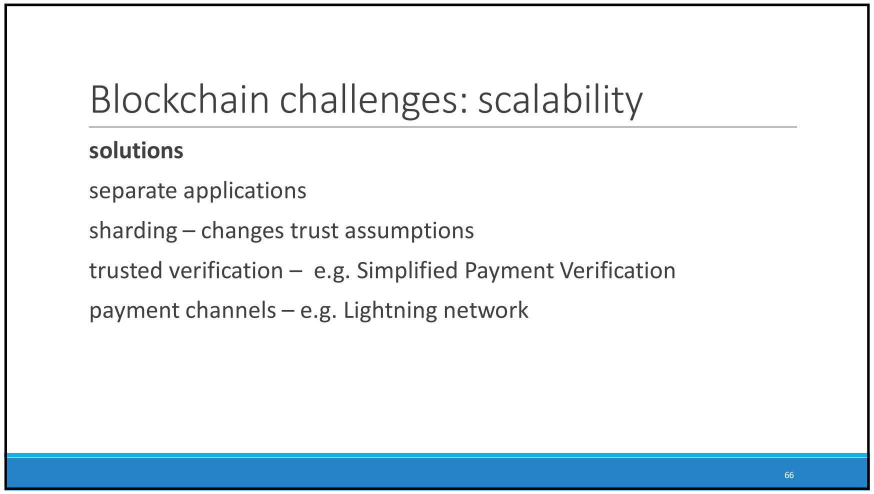
31.5 million transactions/device per year

transaction size: 1 Kbyte

storage: 10^{21} bytes = 1 Zettabyte/year

communications: 256 10^{12} bit/s
= 256 Terabit/s

Cisco (2022 forecast): 587 Exabyte mobile traffic per year (82% is video!)



Blockchain challenges: scalability

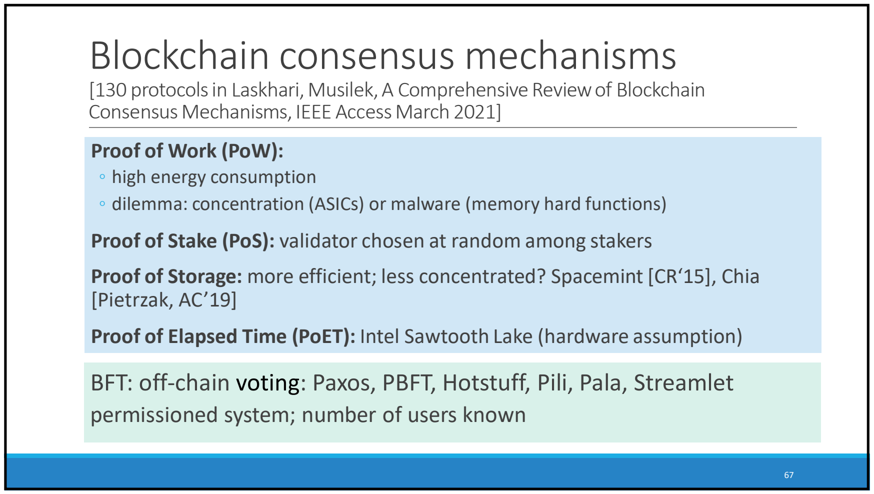
solutions

separate applications

sharding – changes trust assumptions

trusted verification – e.g. Simplified Payment Verification

payment channels – e.g. Lightning network



Blockchain consensus mechanisms

[130 protocols in Laskhari, Musilek, A Comprehensive Review of Blockchain Consensus Mechanisms, IEEE Access March 2021]

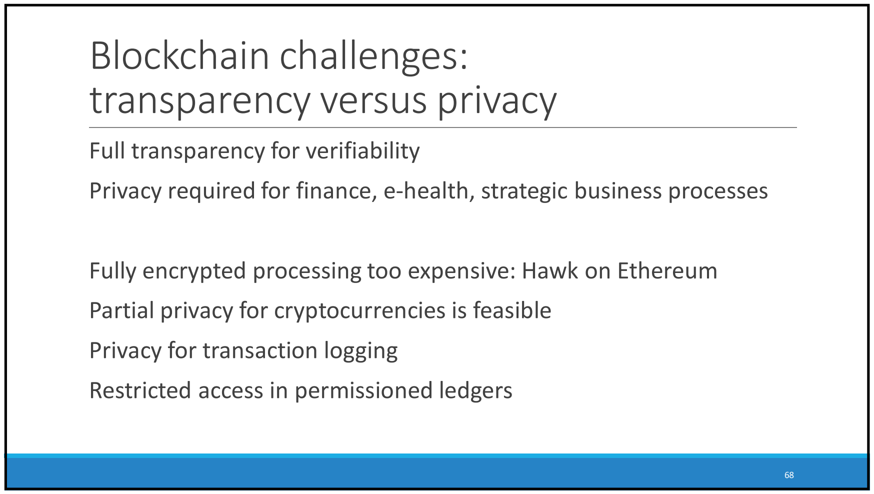
Proof of Work (PoW):
- high energy consumption
- dilemma: concentration (ASICs) or malware (memory hard functions)

Proof of Stake (PoS): validator chosen at random among stakers

Proof of Storage: more efficient; less concentrated? Spacemint [CR‘15], Chia [Pietrzak, AC’19]

Proof of Elapsed Time (PoET): Intel Sawtooth Lake (hardware assumption)

BFT: off-chain voting: Paxos, PBFT, Hotstuff, Pili, Pala, Streamlet
permissioned system; number of users known



Blockchain challenges: transparency versus privacy

Full transparency for verifiability

Privacy required for finance, e-health, strategic business processes

Fully encrypted processing too expensive: Hawk on Ethereum

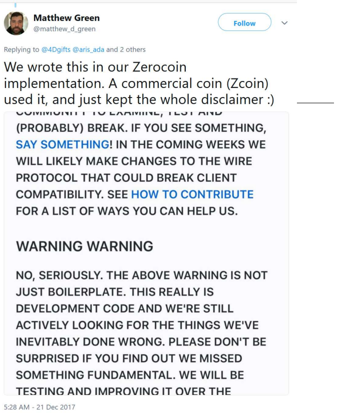
Partial privacy for cryptocurrencies is feasible

Privacy for transaction logging

Restricted access in permissioned ledgers

Adding privacy

Monero:	$ 3071 M
Zcash:	$ 1181 M
Dash:	$ 539 M
Verge:	$ 63 M
Zcoin (!):	$ 49 M?
PIVX:	$ 8 M



Matthew Green
@matthew_d_green

Replying to @4Dgifts @aris_ada and 2 others

We wrote this in our Zerocoin implementation. A commercial coin (Zcoin) used it, and just kept the whole disclaimer :)

COMMUNITY TO EXAMINE, TEST AND (PROBABLY) BREAK. IF YOU SEE SOMETHING, SAY SOMETHING! IN THE COMING WEEKS WE WILL LIKELY MAKE CHANGES TO THE WIRE PROTOCOL THAT COULD BREAK CLIENT COMPATIBILITY. SEE HOW TO CONTRIBUTE FOR A LIST OF WAYS YOU CAN HELP US.

WARNING WARNING

NO, SERIOUSLY. THE ABOVE WARNING IS NOT JUST BOILERPLATE. THIS REALLY IS DEVELOPMENT CODE AND WE'RE STILL ACTIVELY LOOKING FOR THE THINGS WE'VE INEVITABLY DONE WRONG. PLEASE DON'T BE SURPRISED IF YOU FIND OUT WE MISSED SOMETHING FUNDAMENTAL. WE WILL BE TESTING AND IMPROVING IT OVER THE

5:28 AM - 21 Dec 2017

Blockchain challenges: governance of decentralized systems

IT systems tend to evolve toward monopolies or oligopolies
- even open source projects have their “benevolent dictators”

Decentralization is response to mass surveillance and abuses

Decentralization at multiple levels
- transaction approval
- governance (meta-decisions) – today often centralized

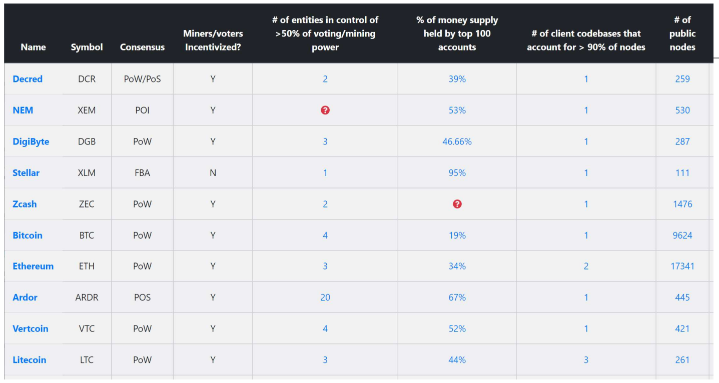
Which decisions to (de-)centralize

Separation of powers

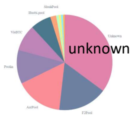
Accountability

Can we learn from centuries of political science?

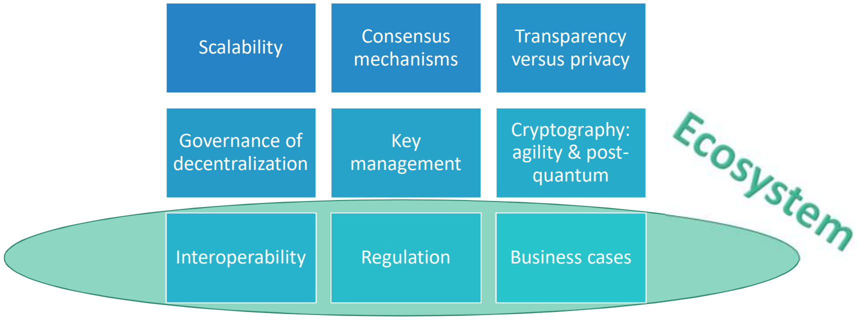
Centralization: https://arewedecentralizedyet.com/



Name	Symbol	Consensus	Miners/voters Incentivized?	# of entities in control of >50% of voting/mining power	% of money supply held by top 100 accounts	# of client codebases that account for > 90% of nodes	# of public nodes
Decred	DCR	PoW/PoS	Y	2	39%	1	259
NEM	XEM	POI	Y	?	53%	1	530
DigiByte	DGB	PoW	Y	3	46.66%	1	287
Stellar	XLM	FBA	N	1	95%	1	111
Zcash	ZEC	PoW	Y	2	?	1	1476
Bitcoin	BTC	PoW	Y	4	19%	1	9624
Ethereum	ETH	PoW	Y	3	34%	2	17341
Ardor	ARDR	POS	Y	20	67%	1	445
Vertcoin	VTC	PoW	Y	4	52%	1	421
Litecoin	LTC	PoW	Y	3	44%	3	261



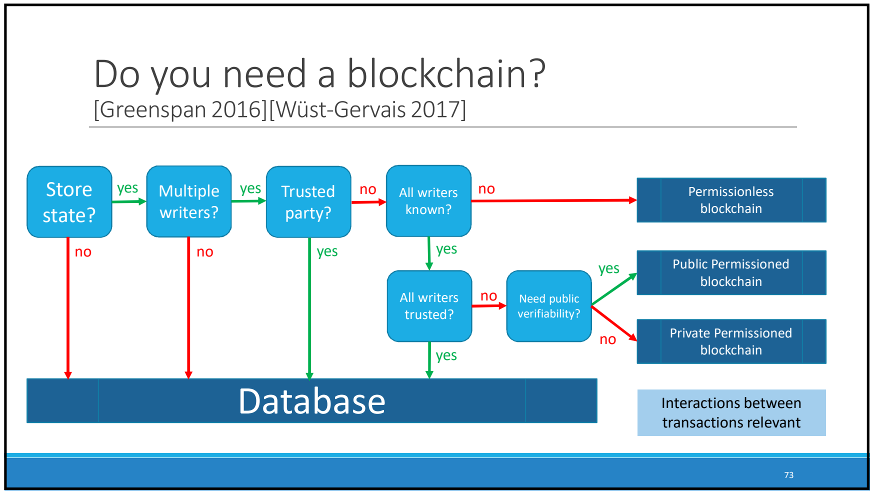
Blockchain challenges



Scalability | Consensus mechanisms | Transparency versus privacy

Governance of decentralization | Key management | Cryptography: agility & post-quantum

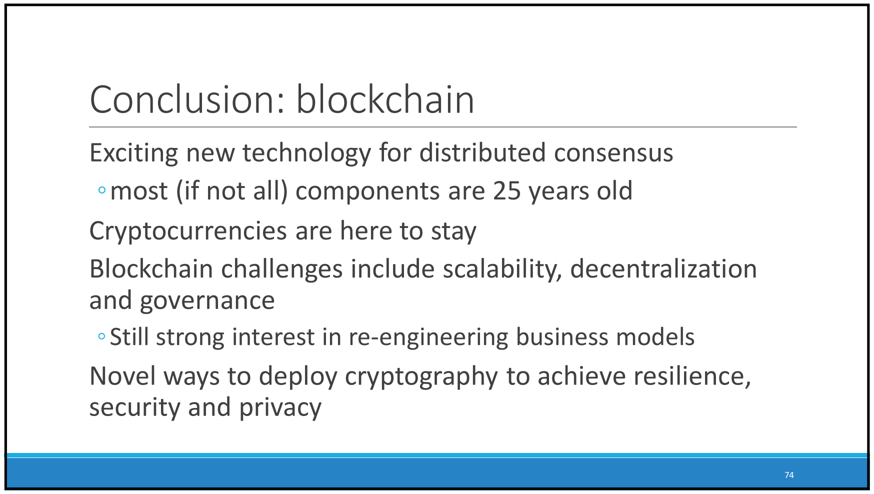
Interoperability | Regulation | Business cases



Do you need a blockchain?

[Greenspan 2016][Wüst-Gervais 2017]

Store state?
yes
Multiple writers?
yes
Trusted party?
no
All writers known?
no
Permissionless blockchain
no
no
yes
yes
All writers trusted?
no
Need public verifiability?
yes
Public Permissioned blockchain
no
Private Permissioned blockchain
yes
Database
Interactions between transactions relevant



Conclusion: blockchain

Exciting new technology for distributed consensus

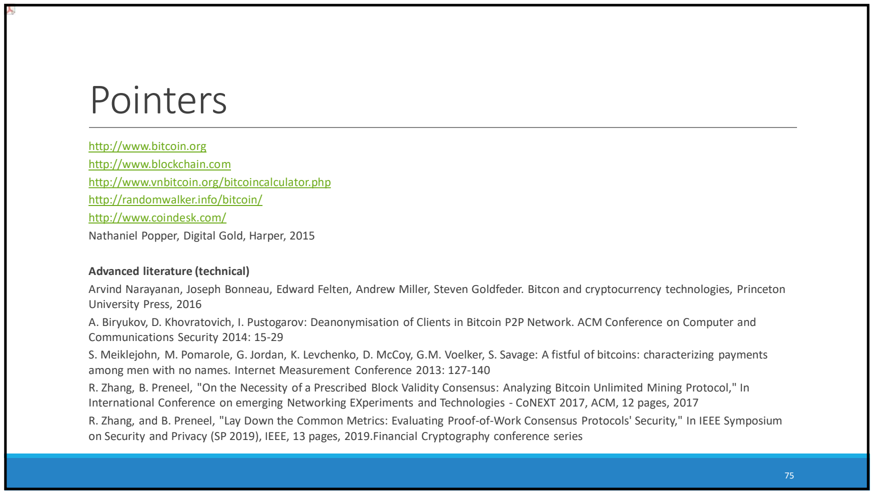
- most (if not all) components are 25 years old

Cryptocurrencies are here to stay

Blockchain challenges include scalability, decentralization and governance

- Still strong interest in re-engineering business models

Novel ways to deploy cryptography to achieve resilience, security and privacy



Pointers

http://www.bitcoin.org
http://www.blockchain.com
http://www.vnbitcoin.org/bitcoincalculator.php
http://randomwalker.info/bitcoin/
http://www.coindesk.com/
Nathaniel Popper, Digital Gold, Harper, 2015

Advanced literature (technical)

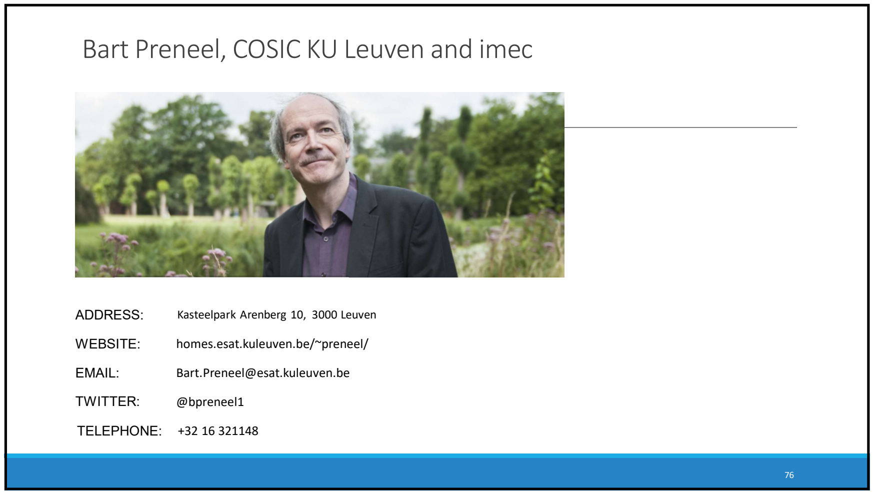
Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. Bitcon and cryptocurrency technologies, Princeton University Press, 2016

A. Biryukov, D. Khovratovich, I. Pustogarov: Deanonymisation of Clients in Bitcoin P2P Network. ACM Conference on Computer and Communications Security 2014: 15-29

S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G.M. Voelker, S. Savage: A fistful of bitcoins: characterizing payments among men with no names. Internet Measurement Conference 2013: 127-140

R. Zhang, B. Preneel, "On the Necessity of a Prescribed Block Validity Consensus: Analyzing Bitcoin Unlimited Mining Protocol," In International Conference on emerging Networking EXperiments and Technologies - CoNEXT 2017, ACM, 12 pages, 2017

R. Zhang, and B. Preneel, "Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security," In IEEE Symposium on Security and Privacy (SP 2019), IEEE, 13 pages, 2019.Financial Cryptography conference series



Bart Preneel, COSIC KU Leuven and imec

ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven
WEBSITE: homes.esat.kuleuven.be/~preneel/
EMAIL: Bart.Preneel@esat.kuleuven.be
TWITTER: @bpreneel1
TELEPHONE: +32 16 321148