Blockchain: Hype or Reality?

PROF. DR. IR. BART PRENEEL COSIC, AN IMEC LAB AT KU LEUVEN, BELGIUM
FIRSTNAME.LASTNAME@ESAT.KULEUVEN.BE

ENISA SUMMER SCHOOL, HERAKLION
17 SEPTEMBER 2019

Outline

A short history of blockchain
Opportunities
What can we learn from PKI?
Challenges
Do you need a blockchain?

History

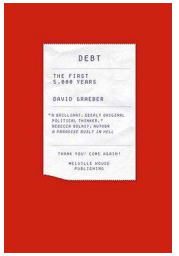
George Santaja (1864-1952)

Those who cannot remember the past are condemned to repeat it

Currencies = maintaining memory

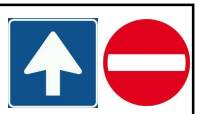
Susa, Iran, ca **3300 BC**

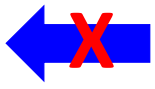
Cuneiform, Sumeria, ca **2600 BC**



Slide inspired by George Danezis

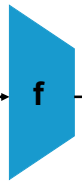
Hash functions (1975): one-way
easy to compute but hard to invert





RIPEMD-160
SHA-256
SHA-512
SHA-3

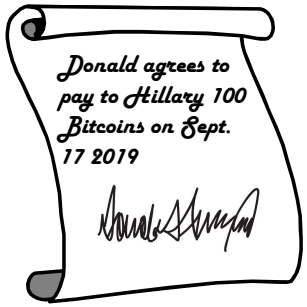
This is an input to a crypto-graphic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs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



1A3FD4128A198FB3CA345932

5

Digital signatures (1975):
"equivalent" to manual signature



Public key

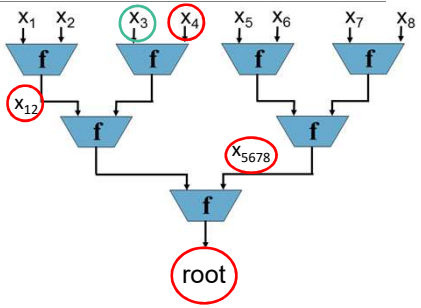
Private key

6

Merkle tree (1979)

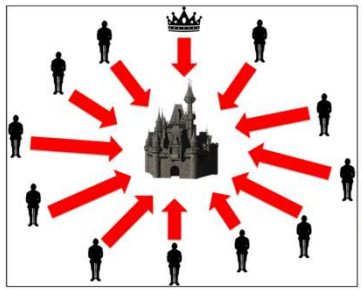
Using a hash function f to authenticate a set of messages through a logarithmic number of values

Applications: digital signatures, revocation…

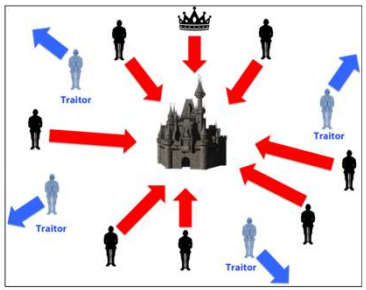


7

Byzantine generals problem (1982)
(can deal with at most 1/3 traitors)



Coordinated Attack Leading to Victory



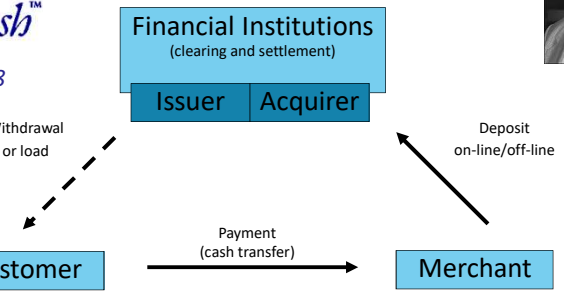
Uncoordinated Attack Leading to Defeat

8

Electronic cash (1985) [David Chaum]

DigiCash™

1990-1998



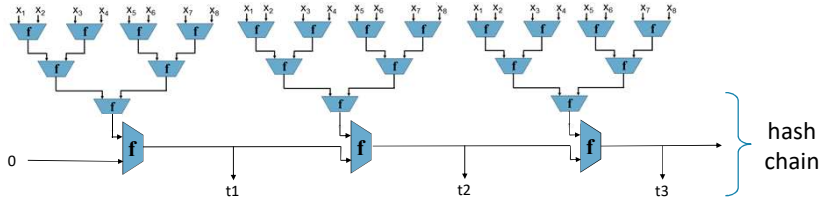
9

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



10

Timestamping: Surety Technologies (°1994)

http://www.surety.com/

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

Estonia: Cybernetica

11

Digital money 1996-2008

e-gold (1996-2008)

- currency backed by real commodity: gold
- centralized ledger of transactions
- becomes a crime magnet (1 million users)
- charges of money laundering and operating without a license
- assets liquidated: $90M in gold

MojoNation (2000-2002)

- peer-to-peer file storage service paid with “Mojo”
- collapsed under hyperinflation
- inspired **BitTorrent** tit-for-tat incentive scheme

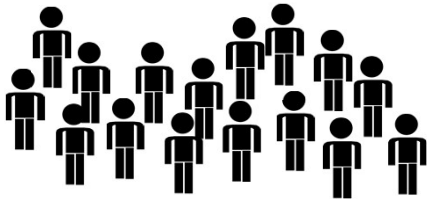
12

Bitcoin (2008): Satoshi Nakamoto

No central bank

Everyone can produce money

Everyone can verify transactions



13

Bitcoin
(paper October 2008 – mining January 2009)

"While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model."

"What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. "

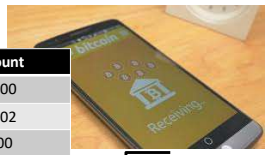
Cryptocurrency with distributed generation and verification of money
Open system where anyone can join

14

Paying with Bitcoin

Donald

Hillary



Block chain

name	amount	
1BxgB4tjcoDnz1LC7bRqyybbE8YNigUQn5	70.00	
19EULTY5DMyvDM6krKtcuvcUoHT4T3QmQL	80.02	
1CMMwinpNduzooWeJ4sK9u7Lkp4YAyK2Lw	5.00	
16PVjaawyWqWnzyttJTAyv7hTcPNmRnVzY	2.50	+1.00
16LNAxwBQupD7yDC8RUSRhyb62BFAZtgae	0.17	
12tQUEb8zzdQSXkgt1553z7zS6Fm1cMQZB	10.00	-1,00
16VT.wYYCLUNgzB8Xs8fYtWWxHR4wdyHm5	2.30	

15

Paying with Bitcoin

Donald

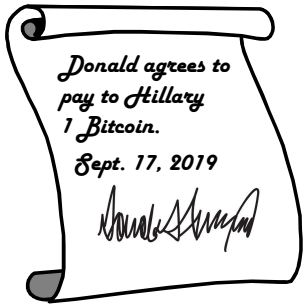
Hillary

Block chain

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

16

Paying with Bitcoin



Public key

12tQUEb8zzdQSXkgt15
53z7zS6Fm1cMQZB

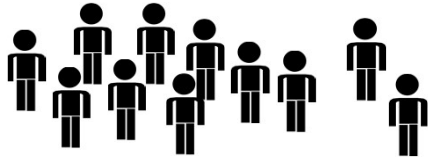
Private key

17

Paying with Bitcoin

Anyone can verify a digital signature

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



18

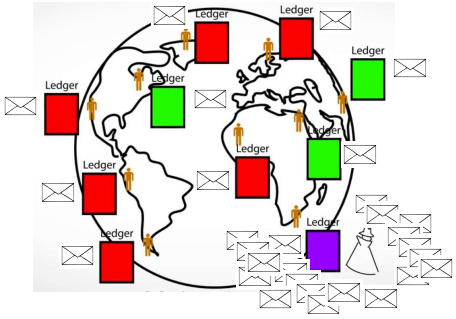
Managing the blockchain

Miners all over the world follow up all the transactions

But due to communication errors or fraud there are multiple versions

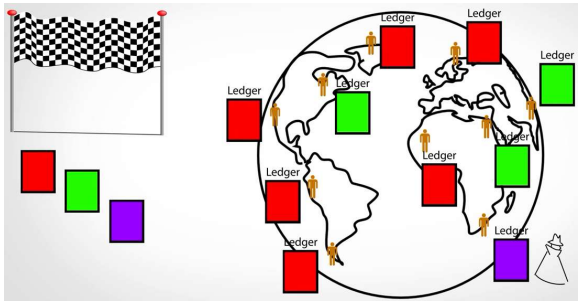
19

Voting? Sybil attack



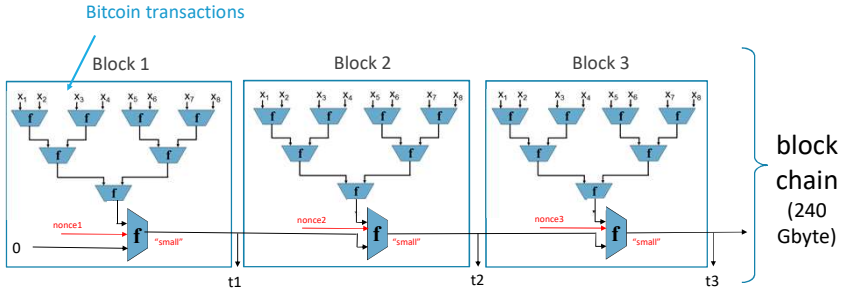
20

Puzzles (a lottery) – [Dwork-Naor'92][Hashcash]



21

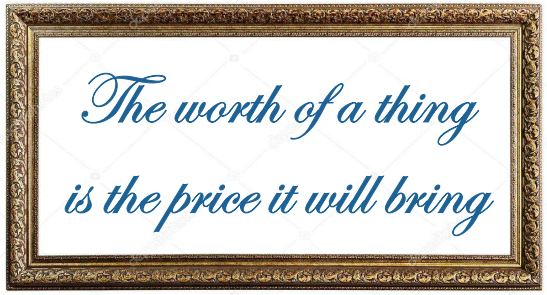
Block Chain: a public decentralized ledger



Also include in every block timestamp and difficulty level of puzzle

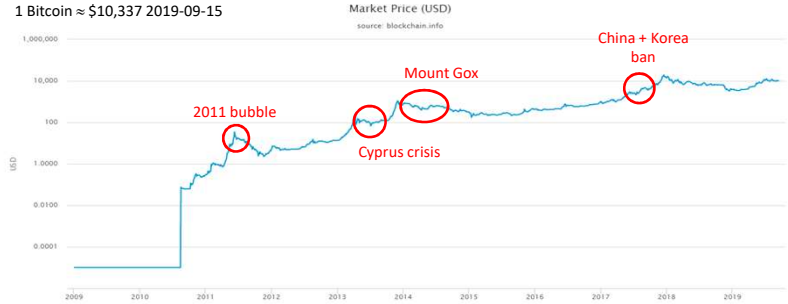
22

Why does Bitcoin have value?



23

Market price in USD (market cap ≈ 185 B$)



24

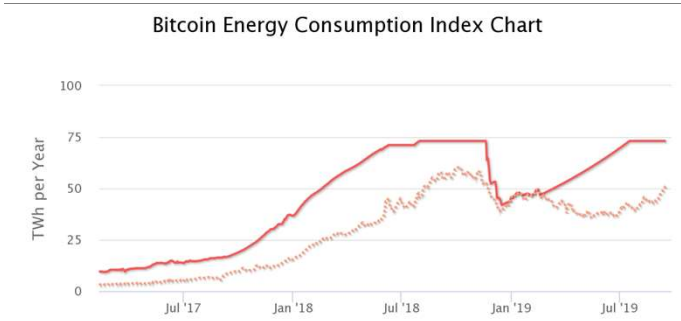
Market price in USD (market cap ≈ 185 B$)

1 Bitcoin ≈ $10,337 2019-09-15

Coinbase has grown from 5.5M to 20+M clients since Jan. 2017

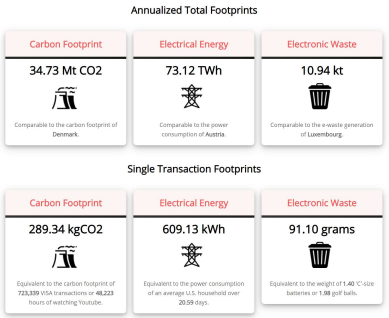
Yet another hack

Energy cost: 50-75 TWh per year (same as Greece)



https://digiconomist.net/

Energy cost: 50-75 TWh per year (same as Greece)



https://digiconomist.net/

Number of transactions per day

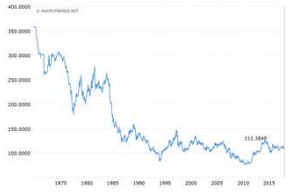
2-5 transactions/s
Peak: 10 transactions/s
large share goes to a few addresses

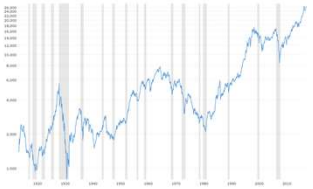
Alipay peak	256.000/s
Visa peak	25.000/s
Western Union peak:	750/s

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





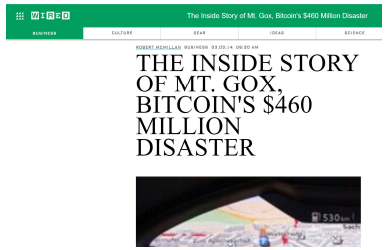
Eli Meregote uses crypto-currencies to send money home to Venezuela

Why are Venezuelans seeking refuge in crypto-currencies?

By Mathew Di Salvo
Technology of Business reporter
15 hours ago | Business

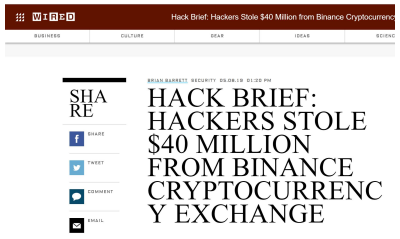
Crypto-currencies have faced a lot of criticism since Bitcoin first came on the scene 10 years ago. But for one group of people, they're proving very useful.

Is Bitcoin is the money of the future?



2013

2019



Total market cap 270 B$

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

Total value of all gold? 7.5 T$
Total value of stock exchange? 70 T$

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)
1	Bitcoin	BTC	$185,389,062,639	$10,335.19	17,937,650	$12,359,022,668
2	Ethereum	ETH	$20,476,086,237	$190.02	107,755,452	$6,333,532,514
3	XRP	XRP	$11,218,174,855	$0.260740	43,024,433,511 *	$894,140,586
4	Bitcoin Cash	BCH	$5,468,656,555	$303.73	18,005,063	$1,246,106,656
5	Litecoin	LTC	$4,445,202,010	$70.27	63,262,367	$2,357,926,009
6	Tether	USDT	$4,118,219,896	$1.00	4,107,544,456 *	$14,872,637,315
7	EOS	EOS	$3,764,046,282	$4.04	931,863,222 *	$1,937,012,724
8	Binance Coin	BNB	$3,241,047,792	$20.84	155,536,713 *	$149,678,900
9	Bitcoin SV	BSV	$2,134,614,875	$119.55	17,854,986	$275,300,683
10	Monero	XMR	$1,296,510,247	$75.33	17,210,096	$58,743,767
11	Cardano	ADA	$1,202,808,429	$0.046392	25,927,070,538	$41,733,140

Facebook libra?

Business and governments

tend to dislike
- distributed control
- full transparency
- unclear governance (or anarchy)
- uncontrolled money supply

restrict
- write, verify or read
- to non-monetary applications

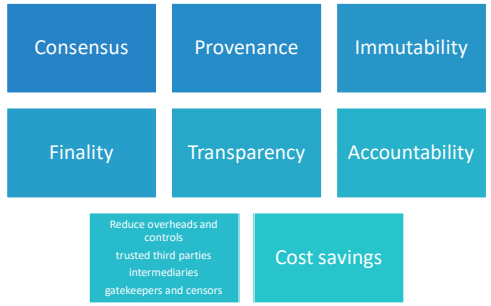
Distributed Ledger: a range of solutions

Public Blockchain	Consortium/Hybrid Blockchain	Fully Private Blockchain

• No central point of control by individuals, corporations or governments
• Permissionless to participate
• Concensus based on "proof of work"
• 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)
		• 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

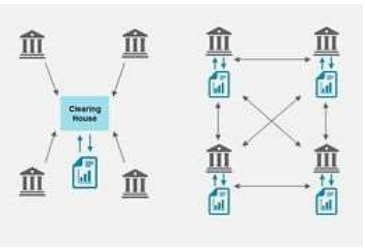
33

Blockchain opportunities



34

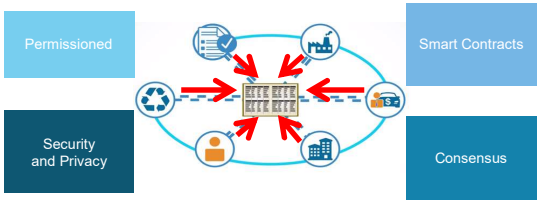
Shared replicated permissioned ledger



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/ 35

Shared ledger



Smart contracts: $300M by 2023 (CACG 32%)

https://www.marketresearchfuture.com/reports/smart-contracts-market-4588

36

Gartner Hype Cycle Emerging Technologies

2003: **PKI** in slope of enlightenment

2014: **cryptocurrencies** just over the peak

2015: idem and crypto exchanges in trough of disillusionment

2016: **blockchain** at the peak

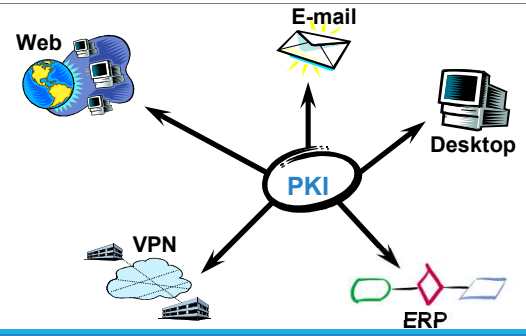
2017: **blockchain** just over the peak

2018: **blockchain** sliding down, but a dedicated hype cycle for blockchain business

2019: only Distributed Autonomous Organization (DAO): innovation trigger

37

The PKI hype (1996-2000): unified security



38

PKI: lessons learned

High stock market valuations: ".com" hype

Single global PKI proposed in the late 1980s

You cannot create trust out of cryptography (few exceptions)

Misaligned incentives invalidate business model: why should users pay for certificates?

Interoperability problems

High integration cost – resistance to change

39

PKI: lessons learned (2): what worked
EMV (1993)

EMV: 7.1 billion cards (55% of total) and 50 million terminals

Highly centralized

Hierarchical trust model

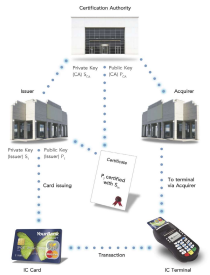


Figure: Cryptomathic

40

PKI: lessons learned (2): what "worked"
SSL/TLS (1995)

SSL/TLS certificates: 660 CAs in browser issued about 60 million server certificates used by 5 billion devices

Browser vendors decide who is included

Users need to trust union of all of the CAs

Trust has been abused by several governments and companies
- e.g. Diginotar

Revocation only implemented in browsers around 2001

Extended Validation (2007) – died around 2018

Recent addition since 2016: Let's Encrypt: 50 million domains
- Price paid: limited checking

41

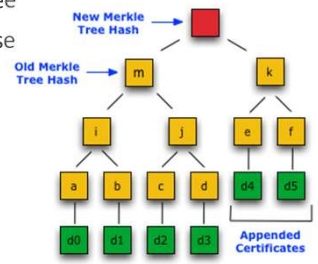
PKI: lessons learned (2): what "worked"
SSL/TLS (1995): certificate transparency (2013)

Certificate transparency: signed Merkle tree

Centralized way to detect mistakes or abuse by CAs

For social good

Issue: privacy



42

PKI summary

EMV: transferring existing power structure online worked

TLS/SSL: after 25 years we are still trying to fix the trust issues
- Example: eTLS (entreprise TLS), published by ETSI in Nov. 2018

43

Blockchain challenges

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

44

Blockchain challenges: scalability

Throughput

Latency

Storage per node

45

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 (1/s)

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!)

46

Blockchain challenges: scalability

solutions

separate applications

sharding – changes trust assumptions

trusted verification – e.g. Simplified Payment Verification

payment channels – e.g. Lightning network

47

Blockchain challenges: consensus mechanism

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

Proof of Stake (PoS): Algorand, Orobouros Praos, Ethereum Casper, Peercoin, Nxt, BlackCoin

Proof of Elapsed Time (PoET): Intel Sawtooth Lake

Consortium with simple voting or Byzantine Fault Tolerance
- central party to appoint members
- or prior agreement on members

48

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: Opacity

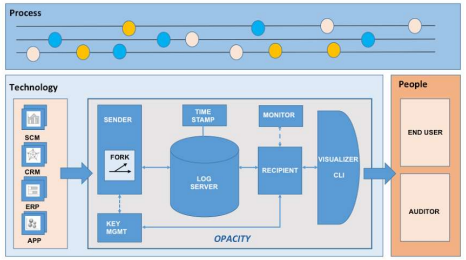
Restricted access in permissioned ledgers

49

Distributed logging + privacy

OPACITY

http://www.project-opacity.com/



50

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

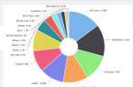
Accountability

Can we learn from centuries of political science?

51

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
Bitcoin	BTC	PoW	Y	4	19%	1	9624
Ethereum	ETH	PoW	Y	3	34%	2	17341
XRP	XRP	RPCA (voting system)	N	2	81%	1	789
Bitcoin Cash	BCH	PoW	Y	3	24.12%	2	2124
Stellar	XLM	FBA	N	1	95%	1	111
Litecoin	LTC	PoW	Y	3	44%	3	261
Cardano	ADA	PoS	N	1	40%	1	1
Monero	XMR	PoW	Y	3	?	1	1691
Dash	DASH	PoW	Y	4	14.65%	1	4649
IOTA	MIOTA	Tangle (DAG)	Y	1	62%	1	484
Neo	NEO	DBFT	N	1	70%	2	46
Ethereum Classic	ETC	PoW	Y	2	?	2	?



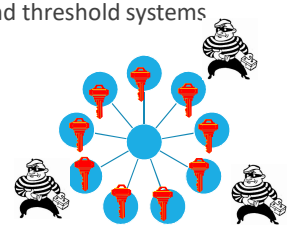
52

Blockchain challenges: key management

Cryptography reduces protection of information to that of keys

Critical information requires better key management

Strong potential for secret sharing and threshold systems



53

Blockchain challenges: cryptography crypto agility

Most blockchains have fixed crypto algorithms

Update requires hard fork

Exceptions
- Crypto in smart contracts
- Hyperledger Fabric: plug-in consensus mechanism

54

Blockchain challenges: cryptography quantum threat

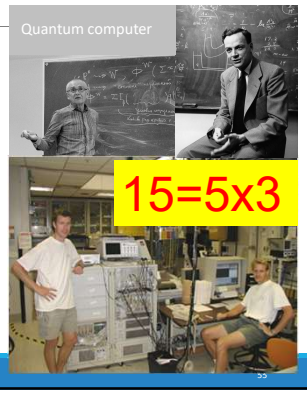
Yuri Manin 1980

Richard Feynman 1981

Exponential parallelism

First trials in the 1990s

7-bit quantum computer in 2001



55

If a large quantum computer can be built

Half of modern cryptography (public-key cryptography) has to be replaced [Shor 1994]
RSA, Diffie-Hellman (including elliptic curves)

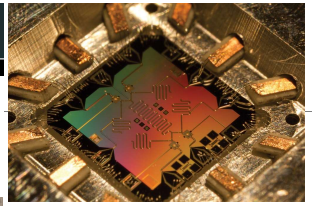
symmetric key sizes: x2 [Grover 1996]

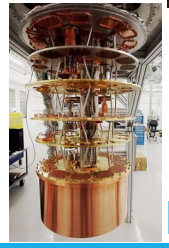

New Scientist

HOME NEWS TECHNOLOGY SPACE PHYSICS HEALTH EARTH HUMANS LIFE TOPICS EVENTS JOBS

Revealed: Google's plan for quantum computer supremacy

The field of quantum computing is undergoing a rapid shake-up, and engineers at Google have quietly set out a plan to dominate





IBM 2017: 50 qubits

Google 2018: 72 qubits
RSA-1024 would require 2048 ideal qubits or 1.5 million real qbits

Rigetti 2018: 128 qubits

http://www.qubitcounter.com/

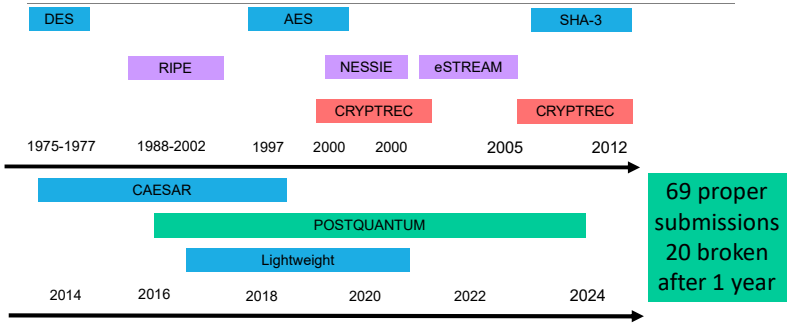
When to switch to quantum resistant cryptography? [Mosca]

Q = #years until first large quantum computer
x = #years it takes to switch (3-10 years)
y = #years data needs to be confidential (10 years)

Need to start switching in the year
2019 + Q – x – y
e.g. Q = 15, x=5, y=10: today!

For data and entity authentication: y = small & defense-in-depth

Open competitions



69 proper submissions
20 broken after 1 year

http://csrc.nist.gov/groups/ST/post-quantum-crypto/index.html

Submissions to NIST non-competition

https://en.wikipedia.org/wiki/Post-Quantum_Cryptography_Standardization

	Signatures	Encryption/KEM	TOTAL
Lattice	3/4	9/24	12/28
Code	0/5	7/19	7/24
Multivariate	4/7	0/6	4/13
Hash	1/4	0	1/4
Other	1/3	1/10	2/13
TOTAL	9/23	17/59	26/82

January 30, 2019: 26 remaining
including LUOV and SABER from KU Leuven

Blockchain challenges: interoperability

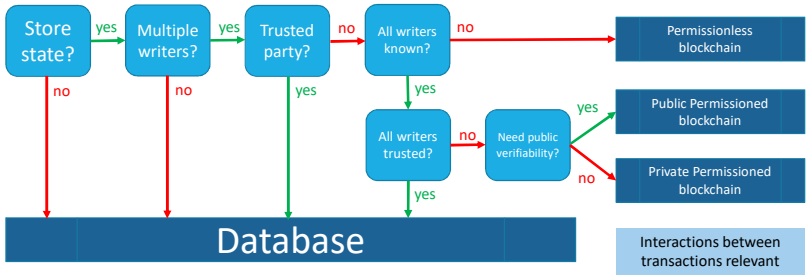
Sidechains for interactions between chains – require further study

Oracles for interaction with physical world
- e.g. Town Crier, Oraclize

61

Do you need a blockchain?

[Greenspan 2016][Wüst-Gervais 2017]



62

Conclusion: blockchain

Exciting new technology for distributed consensus
- most (if not all) components are 25 years old

Many challenges including scalability, decentralization and governance

But still strong interest in re-engineering business models

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

63

Bart Preneel, COSIC an imec lab at KU Leuven

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

?

64