

Behind the scenes of blockchain, cryptocurrencies, and smart contracts



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

FEBRUARY 2019

1

Outline

---

Background  
Bitcoin  
Blockchain  
Business cases

2

Currencies = maintaining memory

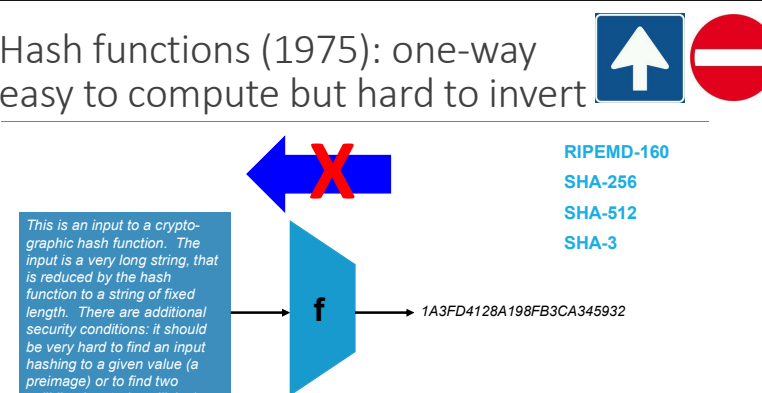


Susa, Iran, ca 3300 BC

Cuneiform, Sumeria, ca 2600 BC

Slide inspired by George Danezis

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

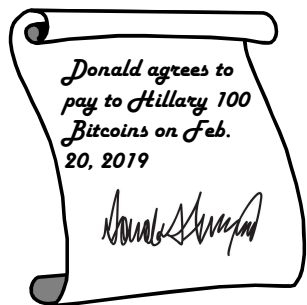


RIPEMD-160  
SHA-256  
SHA-512  
SHA-3

1A3FD4128A198FB3CA345932

4

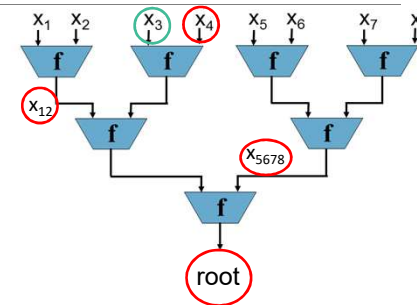
### Digital signatures (1975): "equivalent" to manual signature



5

### Merkle tree (1979)

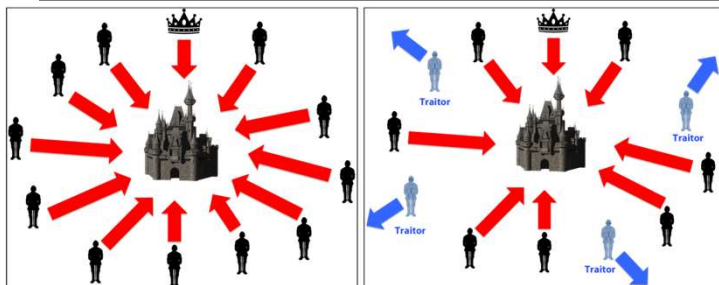
Using a hash function  $f$  to authenticate a set of messages through a logarithmic number of values



Applications: digital signatures, revocation...

6

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



Coordinated Attack Leading to Victory

Uncoordinated Attack Leading to Defeat

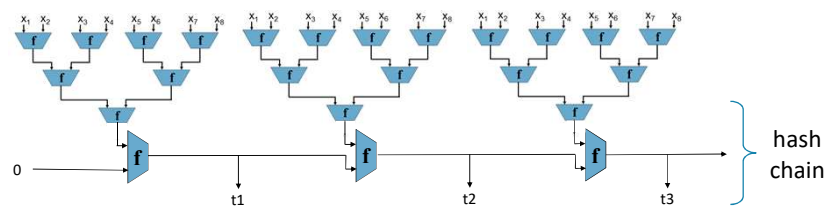
7

### 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



8

## Timestamping: Surety Technologies (°1994)

<http://www.surety.com/>



[https://www.belspo.be/belspo/organisation/Publ/pub\\_ostc/NO/rNOB007\\_en.pdf](https://www.belspo.be/belspo/organisation/Publ/pub_ostc/NO/rNOB007_en.pdf)  
Belgian TIMESEC project (1996-1998)

Estonia: Cybernetica

9

## 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

10

## 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

11

## Paying with Bitcoin

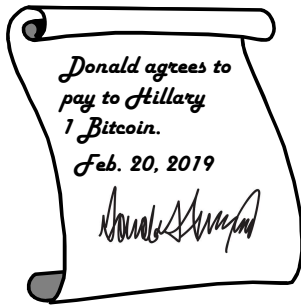
Donald

Hillary

Block chain	
name	amount
1BxgB4tjcoDnz1LC7bRqyybbE8YNigUQn5	70.00
19EULTY5DMyvDM6krKtcuvcoHT4T3QmQL	80.02
1CMMwipNduzooWeJ4sK9u7Lkp4YAyK2Lw	5.00
16PVjaawyWqWnzytTJAyv7hTcPNmRnVzY	3.50
16LNAxwBQupD7yDC8RUSRhyb62BFAZtgae	0.17
12tQUeB8zdzQsXkgT1553z7z56Fm1cMQZB	9.00
16VTrwYYCLUNgzB8Xs8fYtWWxHR4wdyHm5	2.30


12

### Paying with Bitcoin: digital signature (1975)



**Public key**  
12tQUEb8zdzdQ5Xkgt15  
53z7z56Fm1cMQZB

**Private key**


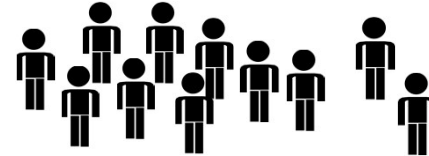


Bitcoin Network

13

### Paying with Bitcoin

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



Bitcoin Network

14

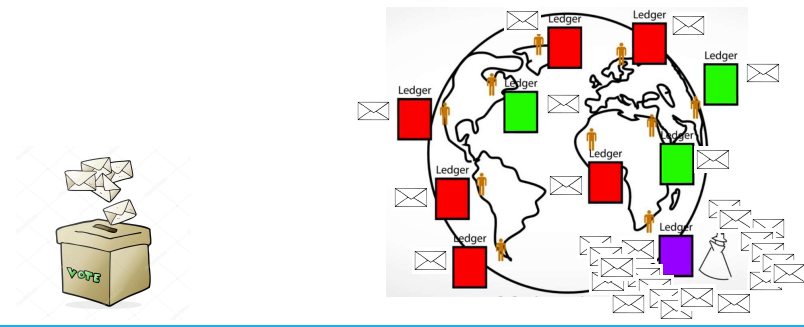
### Managing the blockchain

Miners all over the world follow up all the transactions  
But due to communication errors or fraud there are multiple versions



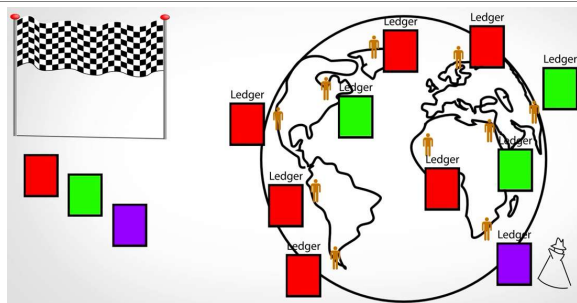
15

### Voting?



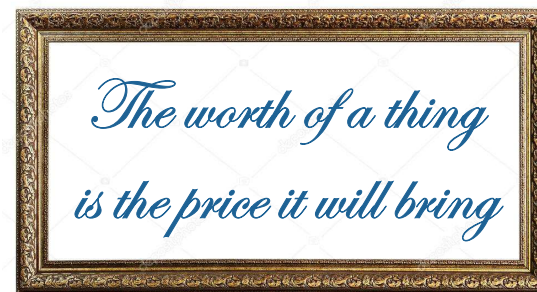
16

### Puzzles (a lottery)



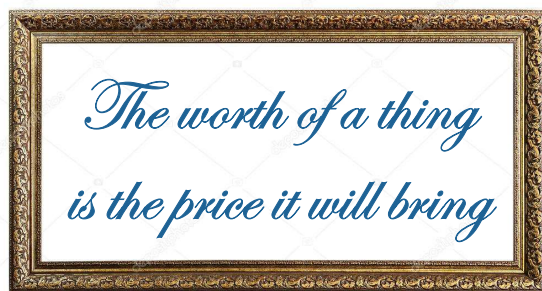
17

### Why does Bitcoin have value?



18

### Why does Bitcoin have value?



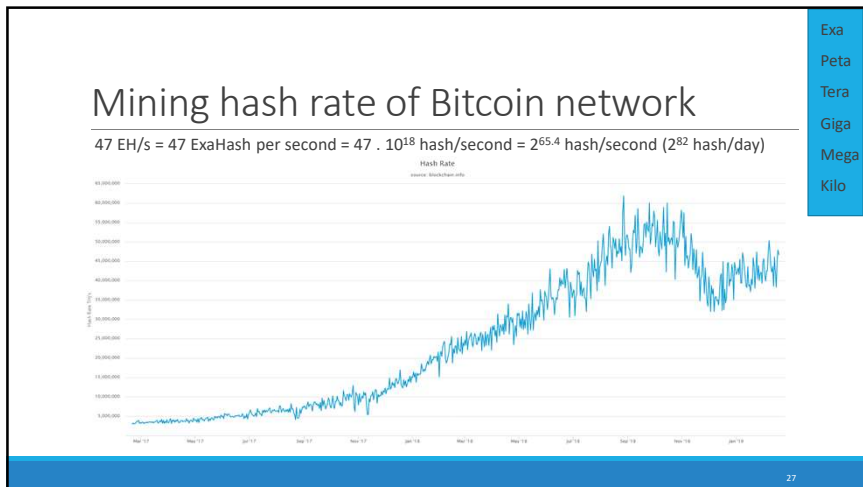
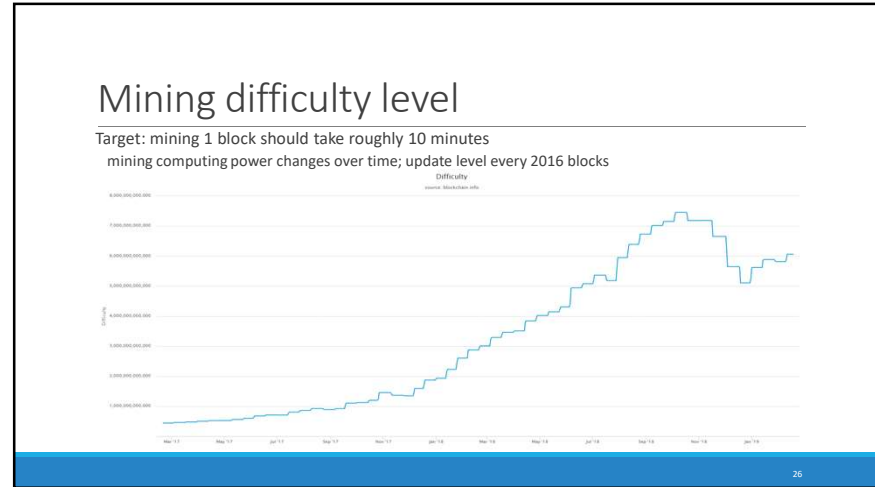
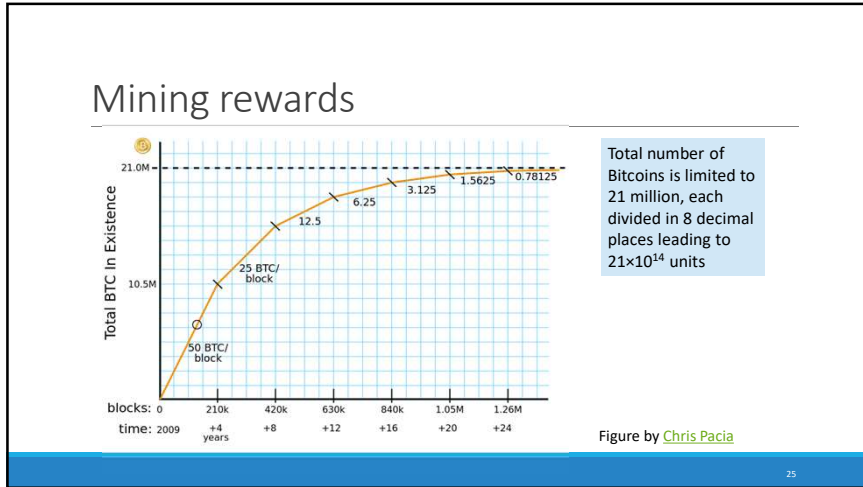
19

### Market price in USD (market cap $\approx$ 68.7 B\$)



20



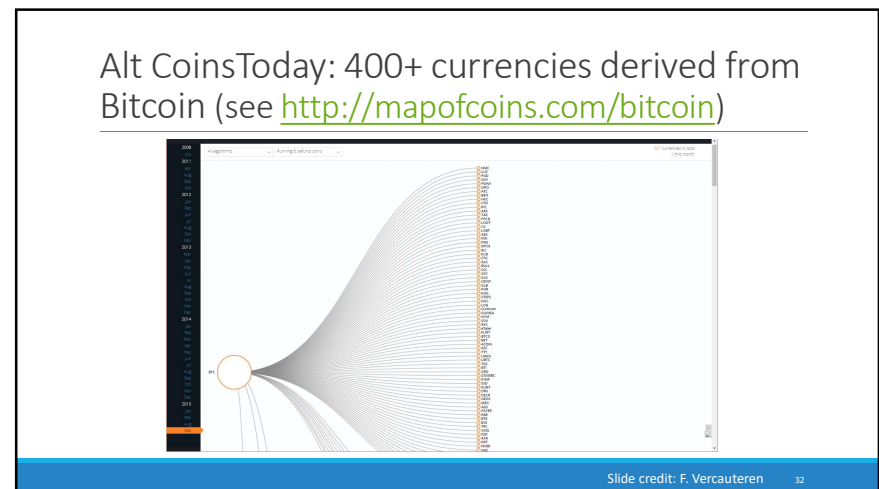
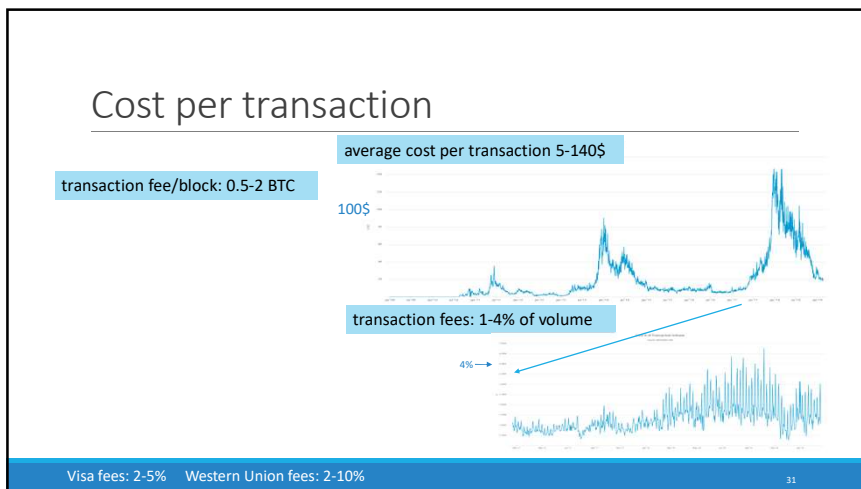
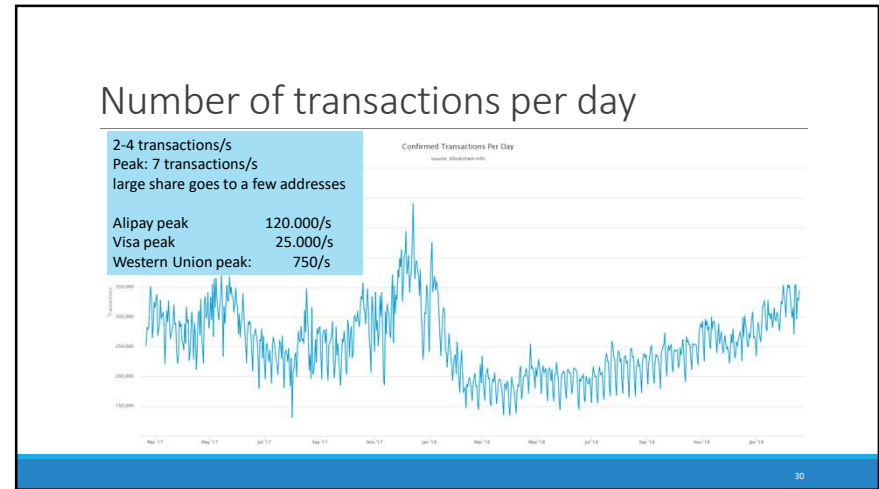
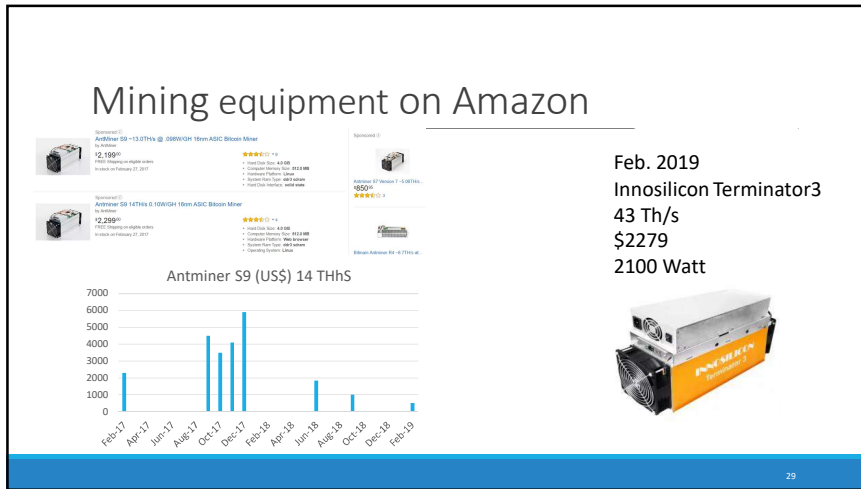


### Mining has become industrial

CPU GPU FPGA ASIC

gold pan sluice box placer mining pit mining

Slide credit: Joseph Bonneau





### Adding privacy

Monero:	\$ 870M
Dash:	\$ 751M
Zcash:	\$ 326M
Verge:	\$ 97M
PIVX:	\$ 45M
Zcoin (!):	\$ 38M

**Matthew Green** (@matthew\_g\_green) · Follow

Replying to @40gfh, @eric\_ada and 2 others

We wrote this in our Zerocoin implementation. A commercial coin (Zcoin) used it, and just kept the whole disclaimer :)  
TRANSPARENCY IS THE SUPERPOWER. I SAID IT FIRST.

**(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

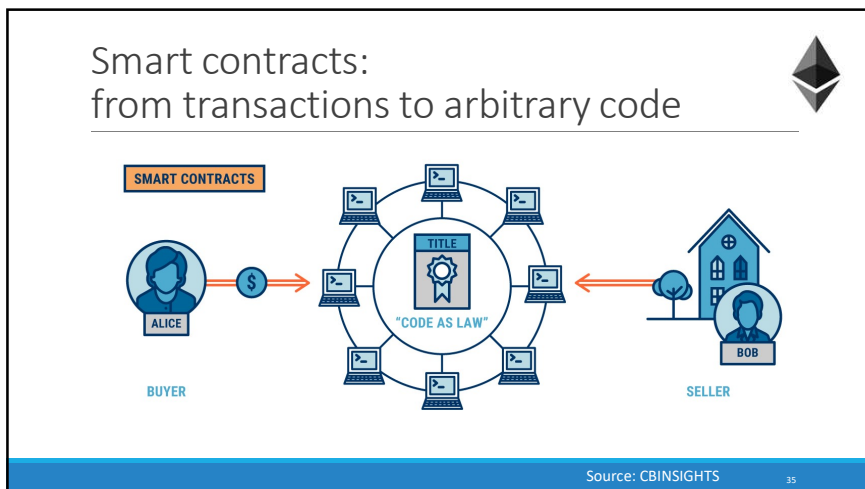
## Total market cap 134 B\$

<https://coinmarketcap.com/all/views/all/> 2070 cryptocurrencies

Total value of all gold? 7.5 T\$

Total value of stock exchange? 70 T\$

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	\$68,878,868,780	\$3,925.43	17,546,837	\$10,411,813,715	0.13%	4.01%	8.05%
2	Ethereum	ETH	\$15,440,383,001	\$147.18	104,820,825	\$5,591,412,419	0.19%	5.53%	21.83%
3	XRP	XRP	\$13,932,250,661	\$0.338095	41,208,983,050	\$1,157,754,572	1.41%	8.90%	12.10%
4	EOS	EOS	\$3,222,121,834	\$3.56	906,245,118	\$2,388,223,959	1.15%	18.02%	27.47%
5	Litecoin	LTC	\$2,915,687,858	\$48.16	60,536,900	\$1,508,222,137	1.03%	7.00%	11.12%
6	Bitcoin Cash	BCH	\$2,583,093,984	\$146.51	17,630,363	\$732,317,507	0.40%	11.81%	20.51%
7	Tether	USDT	\$2,038,552,202	\$1.01	2,021,459,017	\$9,915,591,488	0.03%	0.48%	0.59%
8	TRON	TRX	\$1,697,793,988	\$0.025461	66,682,072,191	\$221,453,969	0.96%	5.24%	4.05%
9	Stellar	XLM	\$1,685,679,658	\$0.007908	19,175,501,080	\$144,190,972	0.89%	9.30%	13.65%
10	Binance Coin	BNB	\$1,362,869,136	\$9.65	141,175,490	\$79,681,257	0.31%	3.21%	3.46%
11	Cardano	ADA	\$1,208,503,894	\$0.046612	25,927,070,538	\$47,091,402	0.73%	8.24%	13.67%
12	Bitcoin SV	BSV	\$1,207,522,411	\$68.50	17,629,186	\$183,744,237	0.85%	6.45%	5.08%
13	Monero	XMR	\$889,560,359	\$51.75	16,803,331	\$58,633,951	-0.38%	5.13%	7.48%
14	IOTA	MIOTA	\$841,097,484	\$0.302604	2,779,530,283	\$22,523,157	-0.05%	6.26%	12.49%



## 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 swaps...

Decentralized Turing-complete virtual machine


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

Quorum: permissioned ledger developed by Morgan-Stanley on top of Ethereum

## Ethereum (ETH) (compared to Bitcoin)



block time of 12 s (600 s)

memory hard algorithm based on Keccak-256 – almost SHA-3 (SHA-256 on ASICs)

70 transactions per block (2000-2500)

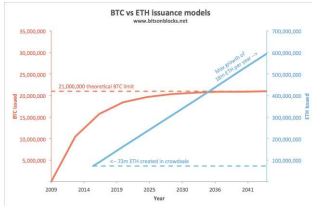
smart contracts (limited scripting)

more complex reward scheme, linear volume (decreasing to limit of 21 million BTC)

- reward 5 ETH per block (12.5 BTC per block but decreasing)
- uncles get reward so no pools (orphans get no reward)

proof-of-work may evolve to proof of stake (no plans)

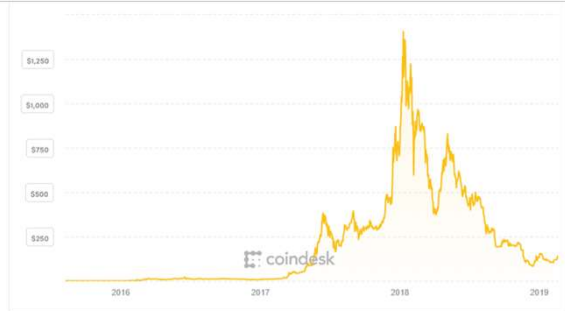
1 ETH =  $10^{18}$  wei (1 BTC =  $10^8$  satoshi)



37

## Ethereum (ETH) graphs

1 ETH = 145\$\$  
142 THash/sec  
Market cap 15 B\$



38

## Some observations on Bitcoin

Bitcoin community aspires to be mainstream but behaves as rebels

- this is not sustainable

Volatile

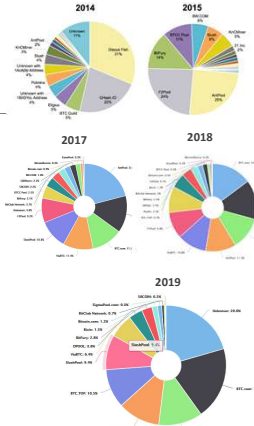
Paying and secure storage somewhat complex

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

All miners are concentrated

Incentives system complex

Not clear that the system will survive, but some ideas will for sure




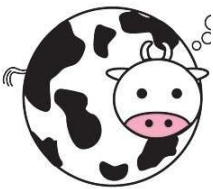
39

## Open issues: Bitcoin

Is Bitcoin incentive compatible?

- Convergence
- Fairness: mining power fraction ~ revenue fraction
- Liveliness
- Sybil attack: attacker controls many nodes in network, can refuse relaying or can favour her own blocks
- Selfish mining attack
- Bribery

Some proofs exist in simplified models e.g. [Garay-Kiayias-Leonardos, Crypto'17]

40

## 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

41

## Outline

Background

Bitcoin

Blockchain

Business cases

42

## Distributed Ledger: a range of solutions

Public Blockchain	Consortium/Hybrid Blockchain	Fully Private Blockchain
<ul style="list-style-type: none"> <li>• No central point of control by individuals, corporations or governments</li> <li>• Permissionless to participate</li> <li>• Consensus based on "proof of work"</li> <li>• Examples:                             <ul style="list-style-type: none"> <li>• Bitcoin</li> <li>• Ethereum</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Controlled by more than two individuals, corporations or governments</li> <li>• Permission on participation from consortium necessary</li> <li>• Arbitrary consensus mechanism</li> <li>• Readability of the blockchain can be public or restricted to the consortium</li> <li>• Example: RSCoin (UCLondon)</li> </ul>	<ul style="list-style-type: none"> <li>• Controlled by one individual, corporation or government (no consensus needed)</li> <li>• Permission on participation from owner necessary</li> <li>• Readability of the blockchain can be public or restricted to one</li> </ul>

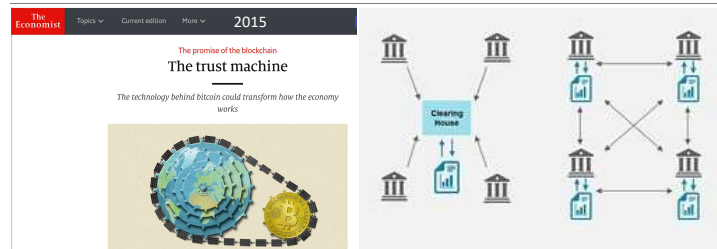
43

## Blockchain opportunities



44

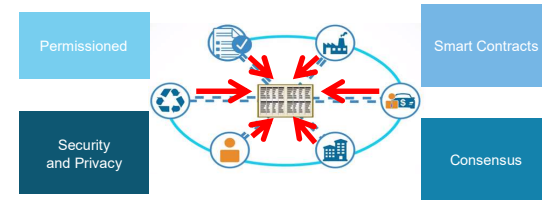
## Shared replicated permissioned ledger



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/> 45

## Shared ledger

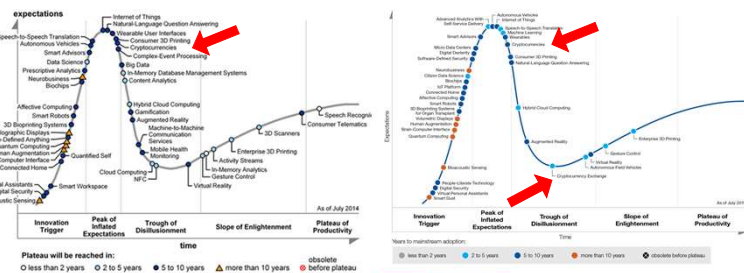


Smart contracts: \$300M by 2023 (CAGR 32%)

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

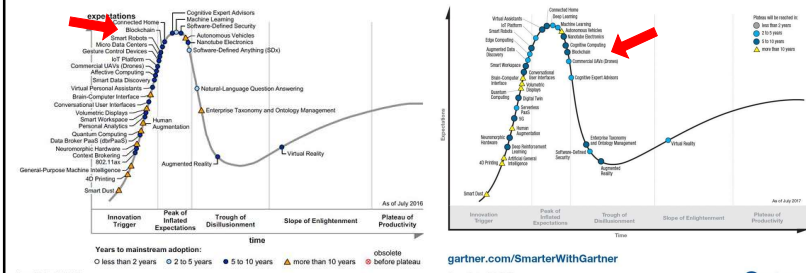
46

## Gartner Hype Cycle Emerging Technologies Cryptocurrencies 2014-2015

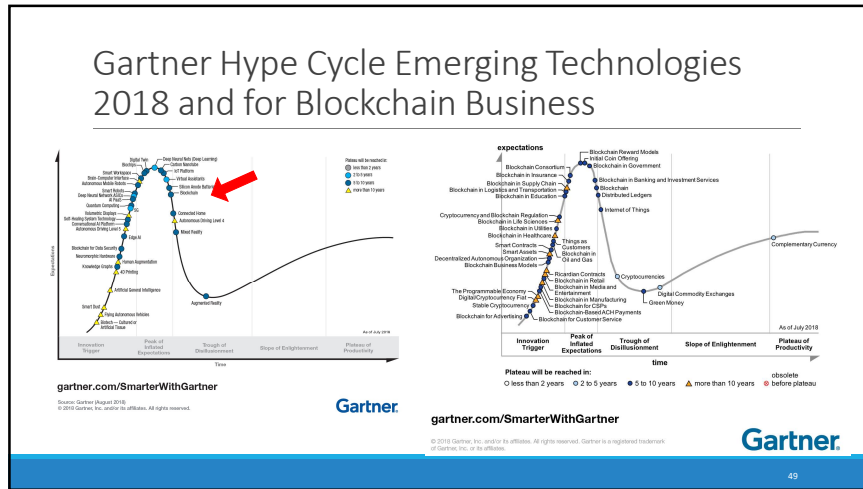


Gartner

## Gartner Hype Cycle Emerging Technologies Blockchain 2016-2017



Gartner



### Blockchain challenges

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

50

### Blockchain challenges: scalability

Throughput  
Latency  
Storage per node

51

### Blockchain challenges: scalability

5 billion users	32 billion IoT devices
1000 transactions/year	31.5 million transactions/device per year
transaction size: 1 Kbyte	transaction size: 1 Kbyte
storage: $5 \cdot 10^{15}$ byte/year = 5 Petabyte/year	storage: $10^{21}$ bytes = 1 Zettabyte/year
	communications: $256 \cdot 10^{12}$ bit/s = 256 Terabit/s

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

52

## Blockchain challenges: scalability

### solutions

- separate applications
- sharding – changes trust assumptions
- trusted verification – e.g. Simplified Payment Verification
- payment channels – e.g. Lightning network

53

## Blockchain challenges: consensus mechanism

### Proof of Work (PoW):

- high energy consumption
- dilemma: concentration (ASICs) or malware (memory hard functions)

Proof of Stake (PoS): Algorand, Ouroboros 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

54

## 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

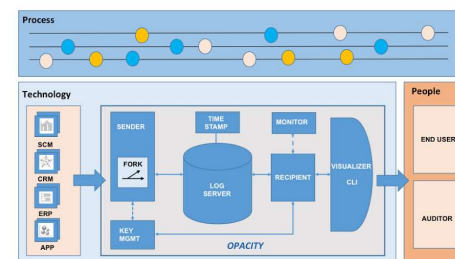
Restricted access in permissioned ledgers

55

## Distributed logging + privacy



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



56

## 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?

57

## 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	MICOTA	Tangle (DAG)	Y	1	62%	1	484
Neo	NEO	DBFT	N	1	70%	2	46
Ethereum Classic	ETC	PoW	Y	2	⚠	2	⚠

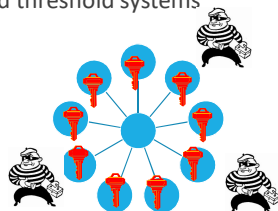
58

## 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



59

## 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

60

## Blockchain challenges: interoperability

Sidechains for interactions between chains – require further study

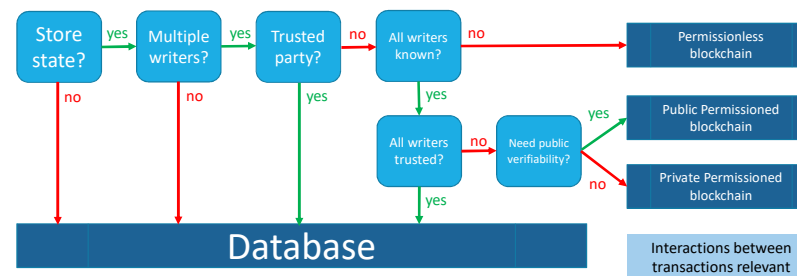
Oracles for interaction with physical world

- e.g. Town Crier, Oraclize

61

## Do you need a blockchain?

[Greenspan 2016][Wüst-Gervais 2017]



62

## Use cases: MERL for development

MERL: Monitoring, Evaluation, Research and Learning

Fall 2018: study of 43 use cases fails to show any benefit

Vendors fail to provide information

63

## World Food

### How Blockchain Is Solving the World Hunger Crisis

Kingston, Nov 26, 2017

By Jason King



It's an unfortunate problem that global hunger and widespread food insecurity can exist on the same planet as unblocked food waste. Yet here we are, 1 out of every 9 people on Earth are food insecure, while 1.3 billion metric tons of food are discarded, lost, wasted. It's entirely unnecessary, but there's a pretty straightforward solution: Get the food where it needs to go to feed the people who are starving.

The World Food Programme's much-publicised "blockchain" has one participant — i.e., it's a database

**The World Food Programme's much-publicised "blockchain" has one participant — i.e., it's a database**

By David Gerard • In: Uncategorized • On Nov 26, 2017 • Comments: 13 • Tags: datarella, devcon, ethereum, houman haddad, joon ian wong, parity, robert opp, world food programme

The World Food Programme is a branch of the United Nations Development Group that helps food security for 80 million people worldwide, particularly in conflict-torn areas.



**World Food Programme**  
wfp.org

WFP blogged in March 2017: "What is 'blockchain' and how is it connected to fighting hunger?" about managing cash disbursements in Pakistan:

The first, successful test at field level of WFP's blockchain innovation—called "Building Blocks"—was carried out in January deep in the heart of Sindh province, Pakistan. As vulnerable families received WFP

64



## Use cases: Forex

---

CLS Services Ltd and IBM Global Financing (IGF)

Foreign exchange trade in more than 140 currencies

2.9 million transactions/year

Dispute resolution: 25,000 cases

Ties up USD 100M for 40 days

Blockchain

- only dealing with dispute resolution
- Dispute resolution in 10 days: 40% improvement in capital efficiency

65

## Use cases: bank X

---

Bank has dozens of payment channels

Internal secure log (blockchain) to detect fraud

66

## 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

Different approaches: <https://www.nervos.org/>

67

Bart Preneel, COSIC an imec lab at KU Leuven



ADDRESS: Kasteelpark Arenberg 10, 3000 Leuven

WEBSITE: [homes.esat.kuleuven.be/~preneel/](https://homes.esat.kuleuven.be/~preneel/)

EMAIL: [Bart.Preneel@esat.kuleuven.be](mailto:Bart.Preneel@esat.kuleuven.be)

TWITTER: @CosicBe

TELEPHONE: +32 16 321148

68