Cryptocurrencies and Distributed Consensus

KU LEUVEN imec embracing a better life

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

9 MAY 2019

1

Outline

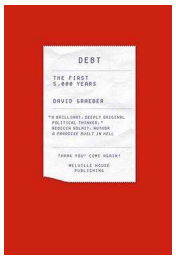
Electronic payments
Secure transactions
Secure execution: contracts
Adding privacy
Permissioned systems
Do I need a blockchain?

2

Currencies = maintaining memory

Susa, Iran, ca **3300 BC**

Cuneiform, Sumeria, ca **2600 BC**



Slide inspired by George Danezis 3

Payment instructions and currencies

Payment Instruments: mechanism of how we transfer value
- cash
- letters of credit
- cheques
- bank transfer
- debit card

Each payment instrument has a cost
- actual monetary cost
- handling cost

Instruments have different security properties
- integrity/authenticity
- privacy: compare cash to bank or credit card payments

Slide credit: George Danezis 4

Cash

bearer instrument

off-line payments

low and medium value

privacy, coins not traceable

widely accepted

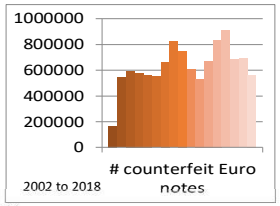
bank: risk of forgery, cost of transport

user: theft and loss, change, physical presence

government: money laundering

5

€/£/$ Counterfeiting



> 22 billion € notes in circulation with value of € 1.2 trillion

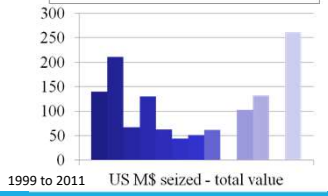
2018: fraudulent: 563,000 or 1 in 39,000

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



1995: $ 15.5 million (1% digitally produced)

2005: $ 61 million (45% digitally produced)

2015: $ 147 million (61% digitally produced)

Fraudulent: 1 to 2 in 10,000

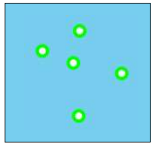
$1.2 trillion genuine in 2015

redesign: 1928, 1990, 1996-2003, 2003-2013

6

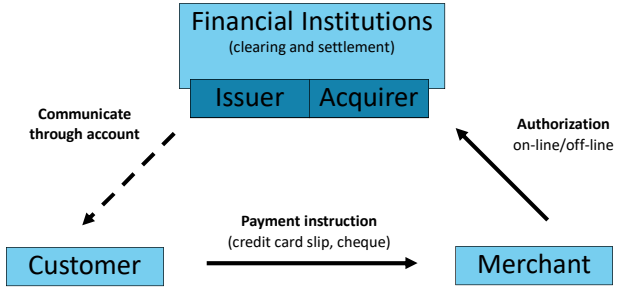
Common features e.g. $/€

pattern detected by scanners and copiers



7

Payment by instruction



8

Payment by instruction

Convenient

Reduced risk

Identify users: manual signatures, magstripe cards, smart cards

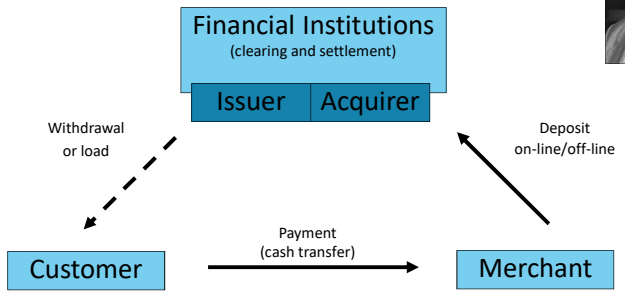
Traceable

Verification expensive:

- credit/debit card: on-line, tamper resistant modules
- check: off-line, delay, processing cost

9

Electronic cash [David Chaum]



10

Electronic cash

DigiCash™ *1990-1998*

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

11

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 12

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

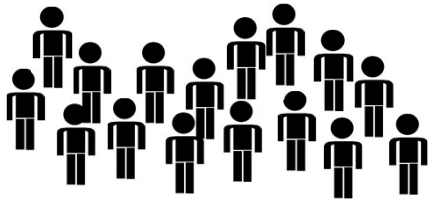
Slide credit: George Danezis 13

Bitcoin (2008): Satoshi Nakamoto

No central bank

Everyone can produce money

Everyone can verify transactions



14

What is Bitcoin? (2008)

E-currency with distributed generation and verification of money

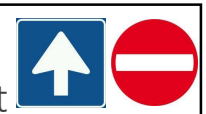
Transactions
- irreversible
- inexpensive
- over anonymous peer-to-peer network
- broadcast within seconds and verified within 10 to 60 minutes by inclusion in hash chain
- double spending prevention using a public decentralized ledger (chaining mechanism)

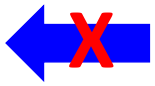
Pseudonymous
- Money is linked to public key – can generate arbitrary key pairs and move money around
- But in many cases identification is possible

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

15

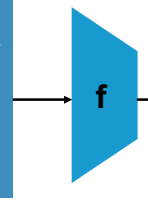
Hash functions (1975): one-way easy to compute but hard to invert





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

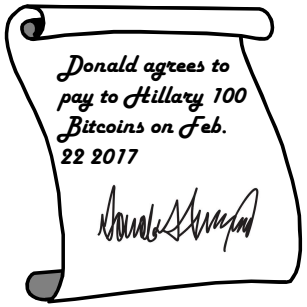
This is an input to a crypto-graphic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs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



1A3FD4128A198FB3CA345932

16

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



Public key

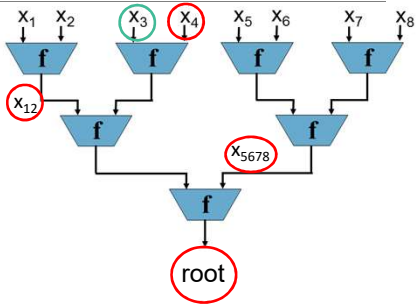
Private key

17

Merkle tree (1979)

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

Applications: digital signatures, revocation…



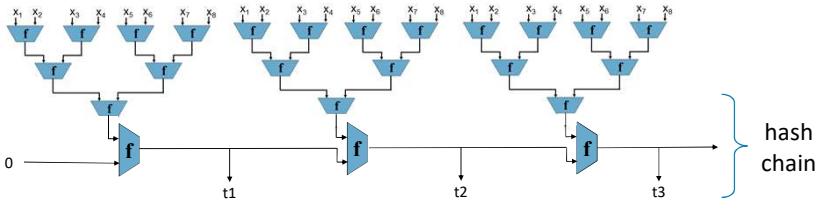
18

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



19

Timestamping: Surety Technologies (°1994)

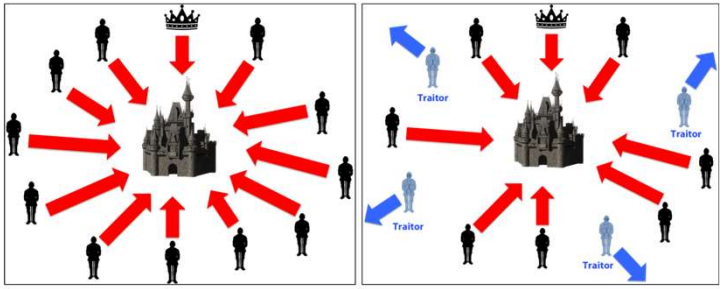
http://www.surety.com/

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

Estonia: Cybernetica

20

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



Coordinated Attack Leading to Victory

Uncoordinated Attack Leading to Defeat

21

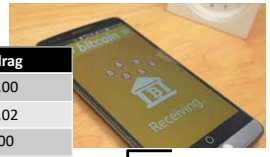
Paying with Bitcoin

Donald

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	

Hillary



22

Paying with Bitcoin

Donald

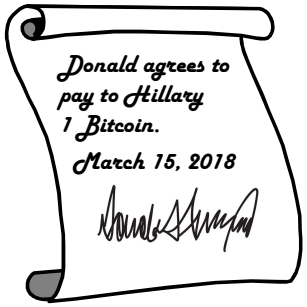
Block chain

naam	bedrag
1BxgB4tjcoDnz1LC7bRqyybbE8YNigUQn5	70,00
19EULTY5DMyvDM6krKtcuvcUoHT4T3QmQL	80,02
1CMMwinpNduzooWeJ4sK9u7Lkp4YAyK2Lw	5,00
16PVjaawyWqWnzyttJTAyv7hTcPNmRnVzY	3,50
16LNAxwBQupD7yDC8RUSRhyb62BFAZtgae	0,17
12tQUEb8zzdQSXkgt1553z7zS6Fm1cMQZB	9,00
16VTrwYYCLUNgzB8Xs8fYtWWxHR4wdyHm5	2,30

Hillary

23

Paying with Bitcoin



Public key

12tQUEb8zzdQSXkgt15
53z7zS6Fm1cMQZB

Private key

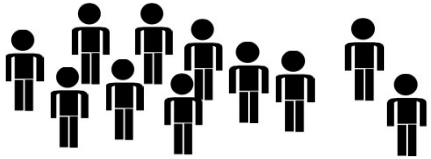
Bitcoin Network

24

Paying with Bitcoin

Anyone can verify a digital signature

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



25

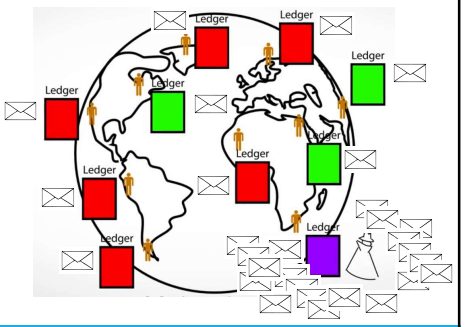
Managing the blockchain

Miners all over the world follow up all the transactions

But due to communication errors or fraud there are multiple versions

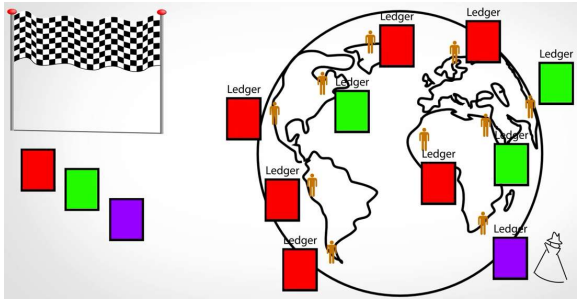
26

Voting? Sybil attack



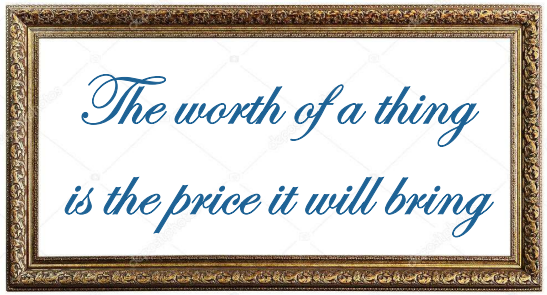
27

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



28

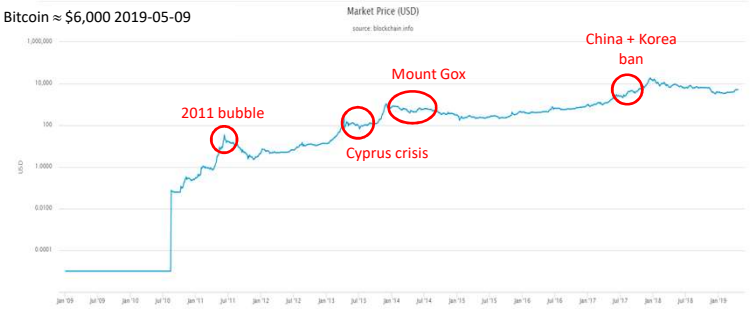
Why does Bitcoin have value?



29

Market price in USD (market cap ≈ 105 B$)

1 Bitcoin ≈ $6,000 2019-05-09



30

Market price in USD (market cap ≈ 105 B$)

1 Bitcoin ≈ $6,000 2019-05-09

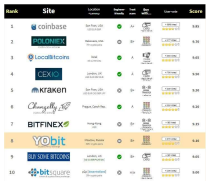
Coinbase has grown from 5.5M to 20+M clients since Jan. 2017

31

How do I get Bitcoin?

ATM

exchange

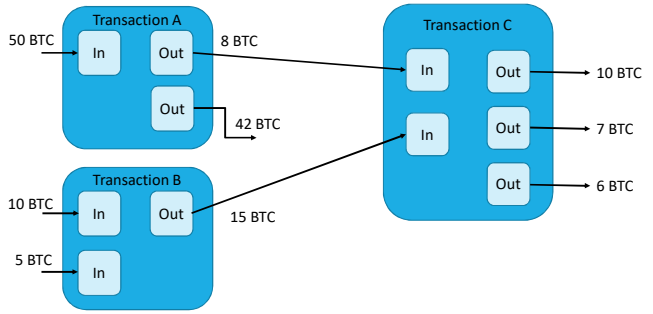


mine at home

Only in theory in 2019

32

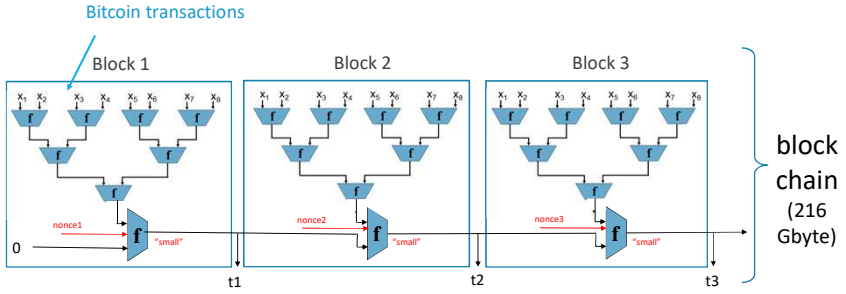
Bitcoin Transaction: send money from one public key (address) to another one



Slide credit: F. Vercauteren

33

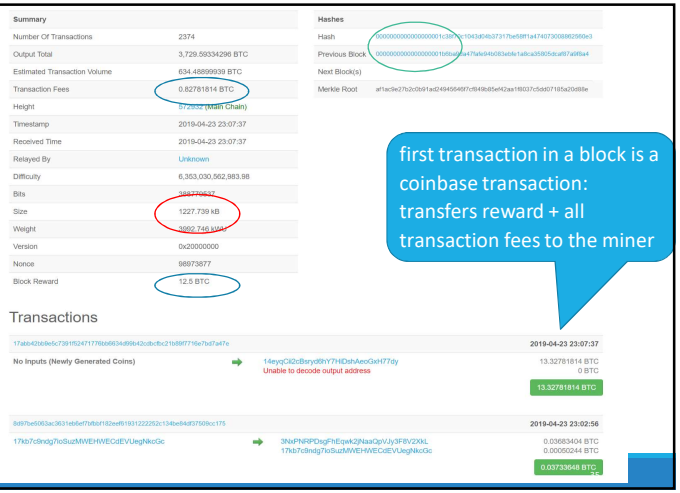
Block Chain: a public decentralized ledger



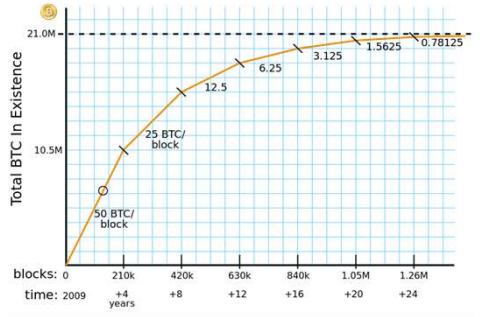
Also include in every block timestamp and difficulty level of puzzle

34

Block #572932



Mining rewards



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

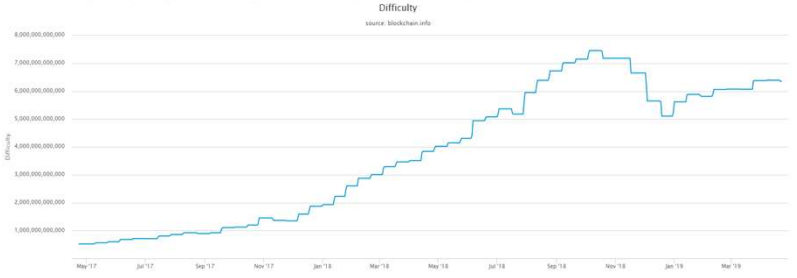
Figure by Chris Pacia

36

Mining difficulty level

Target: mining 1 block should take roughly 10 minutes

mining computing power changes over time; update level every 2016 blocks

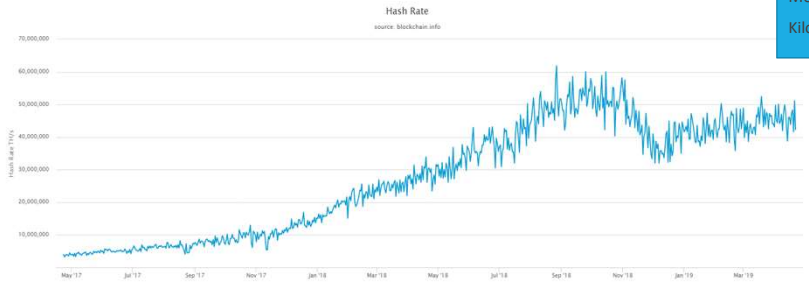


37

Mining hash rate of Bitcoin network

50 EH/s = 50 ExaHash per second = 50 . 10^{18} hash/second = $2^{65.4}$ hash/second (2^{82} hash/day)

Exa
Peta
Tera
Giga
Mega
Kilo

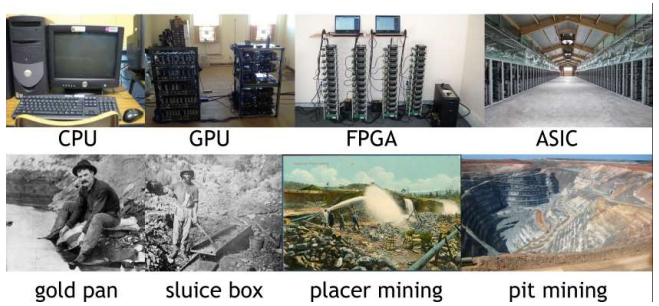


38

Miners revenue (per day): 10 M$

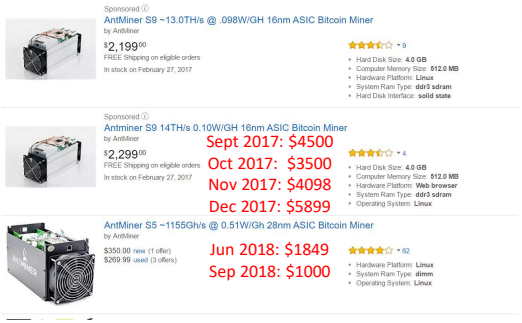
39

Mining has become industrial



Slide credit: Joseph Bonneau 40

Mining equipment on Amazon (Feb. 2017)



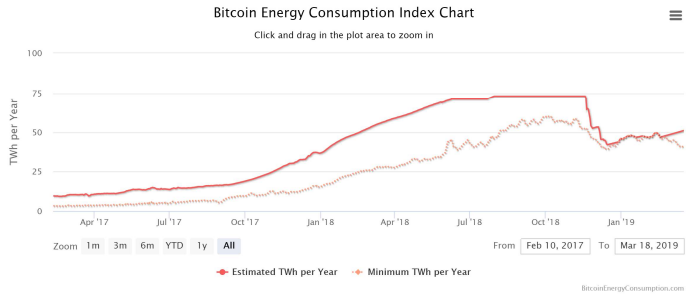
Sept 2017: $4500
Oct 2017: $3500
Nov 2017: $4098
Dec 2017: $5899

Jun 2018: $1849
Sep 2018: $1000

Apr. 2019
Innosilicon T2 Turbo
24 TH/s
$1900
1980 Watt
0.08 W/GH

41

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



https://digiconomist.net/

42

Cost of leaderless consensus

Distributed consensus protocol:

- whichever coalition deploys most hash power, has control of the block chain
- 5 10^{19} hash/second is a significant cost.
- not performing any useful task!

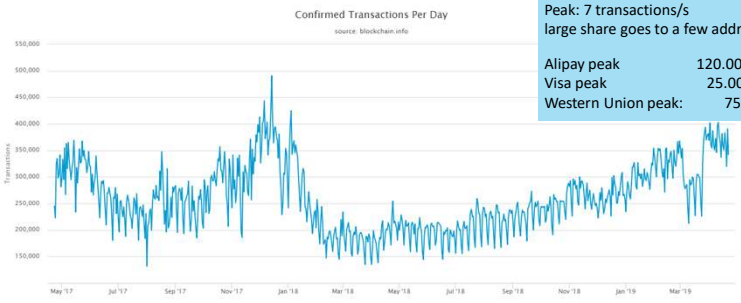
Electricity + Networking costs:

- 0.10-0.20 W/GH/s or 8000 MWatt
- @10 cent per KWh: 1 block costs 25-50K$ electricity (12.5 BTC = +/-70 K$)
- 0.3% of global electricity consumption; 1 transaction "uses" power of 35 US households in a day

Profit calculator: http://www.vnbitcoin.org/bitcoincalculator.php
Energy estimates: https://digiconomist.net/bitcoin-energy-consumption

43

Number of transactions per day



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

Alipay peak	120.000/s
Visa peak	25.000/s
Western Union peak:	750/s

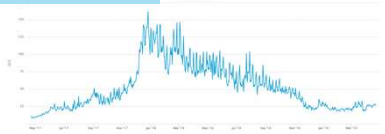
44

Cost per transaction

transaction fee/block: 0.5-2 BTC

average cost per transaction 5-140$

100$



transaction fees: 1-4% of volume

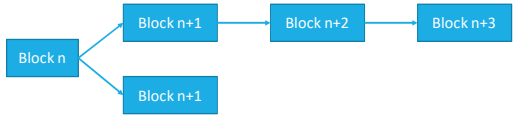
2%

Visa fees: 2-5% Western Union fees: 2-10%

45

Bitcoin (Soft) Forks

Communication error (network split) or attack (see later):

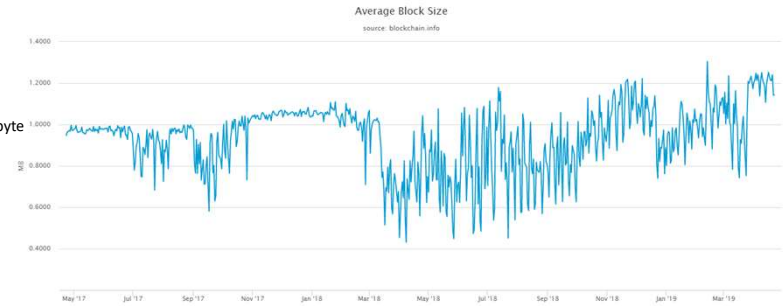


- Miners: work on longest chain (most difficult one)
- If two have same length: choose block that arrived first
- Transactions in orphan blocks are rebroadcast
- Transaction is typically accepted after it is included in 6 blocks (60 minutes)

46

Average block size

1 Mbyte



47

Larger block size?

Higher transaction confirmation throughput

- More transactions with lower fees

But

- higher network bandwidth
- more signature verifications
- more memory to store unspent transaction output (UTXO)

Different implications for miners and public nodes

Resulted in hard forks: Bitcoin cash (Aug'17), Bitcoin Gold (Oct'17) and Bitcoin SV (Nov'18)

48

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 (May'19 216 GByte!)
- Authoritative one is the longest – race for aggregate CPU power

Who has it to start with? (Does it matter?)
- Satoshi Nakamoto

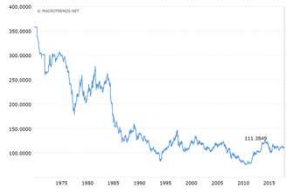
Easy to use? What if something goes wrong?

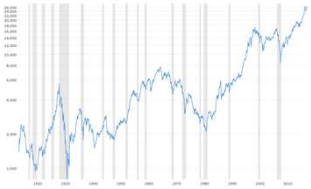
Slide credit: George Danezis 49

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

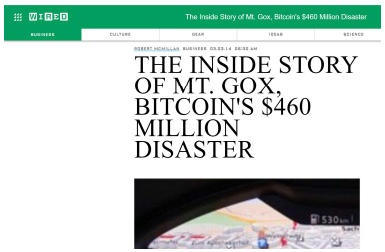
Why are Venezuelans seeking refuge in crypto-currencies?

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.

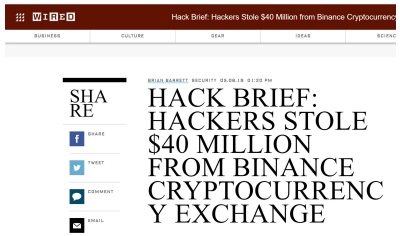
50

Is Bitcoin is the money of the future?



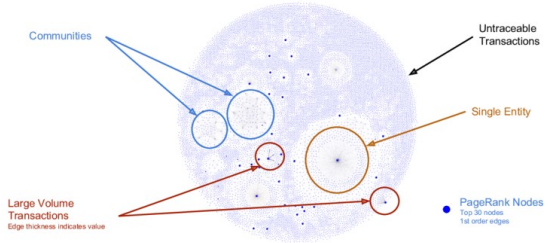
2013

2019



51

Does Bitcoin offer privacy?



Typical Transaction Graph for a day

52

Limits of pseudonymity

- Betcoin gambling site was hacked in April 2012
- 3,171 BTC were stolen in total (2902, 165, 17, and 87 BTC)
- Did not move until March 15 2013 (BTC goes up)
- Aggregated with other small addresses into one large address
- Then began a peeling chain
- After 10 hops, a peel went to Bitcoin-24,
- And in another 10 hops a peel went to Mt. Gox

in total, 374.49 BTC go to known exchanges, all directly off the main peeling chain, which originated directly from the addresses known to belong to the thief.

Slide credit: George Danezis 53

Total market cap 186 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
1	Bitcoin	BTC	$104,802,949,857	$5,924.57	17,689,550
2	Ethereum	ETH	$17,900,318,662	$168.89	105,986,035
3	XRP	XRP	$12,640,887,504	$0.300021	42,133,310,721 *
4	Bitcoin Cash	BCH	$5,045,735,712	$283.93	17,771,238
5	Litecoin	LTC	$4,557,377,344	$73.88	61,683,857
6	EOS	EOS	$4,415,883,710	$4.85	910,788,967 *
7	Binance Coin	BNB	$2,999,198,838	$21.24	141,175,490 *
8	Tether	USDT	$2,773,390,037	$0.998846	2,776,595,295 *
9	Stellar	XLM	$1,796,609,599	$0.093755	19,162,620,760 *
10	Cardano	ADA	$1,669,282,120	$0.064384	25,927,070,538
11	TRON	TRX	$1,653,981,971	$0.024804	66,682,072,191
12	Monero	XMR	$1,132,357,667	$66.73	16,968,509
13	Dash	DASH	$1,031,773,064	$117.29	8,796,672

54

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

55

Ethereum (ETH) (compared to Bitcoin)

block time of 12 s (600 s)

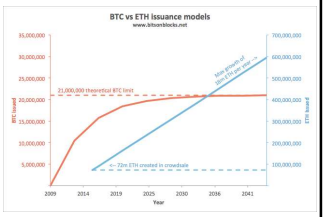
memory hard algorithm based on Keccak-256 – almost SHA-3 (SHA-256 on ASICs)

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)

56

Ethereum (ETH) graphs

1 ETH = 171$
150 THash/sec
Market cap 18 B$

57

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

58

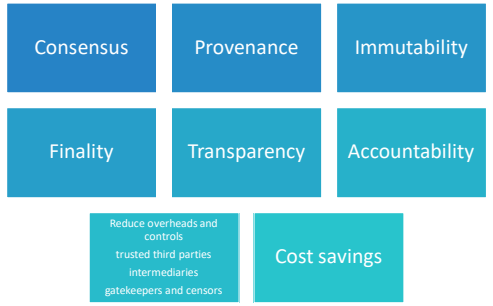
Distributed Ledger: a range of solutions

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

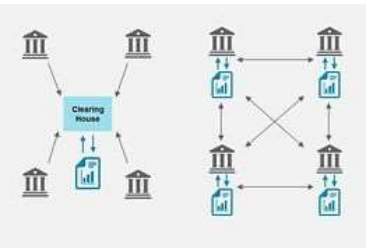
59

Blockchain opportunities



60

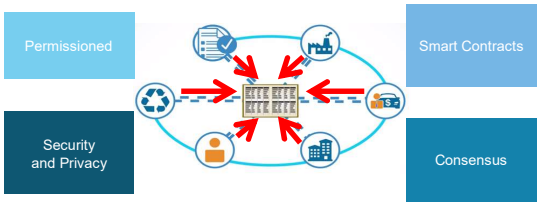
Shared replicated permissioned ledger



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/ 61

Shared ledger



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

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

62

Gartner Hype Cycle Emerging Technologies Cryptocurrencies 2014-2015

63

Gartner Hype Cycle Emerging Technologies Blockchain 2016-2017

64

Gartner Hype Cycle Emerging Technologies 2018 and for Blockchain Business

65

Blockchain challenges

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

66

Blockchain challenges: scalability

Throughput

Latency

Storage per node

67

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

Bitcoin: 1 Mbyte/10 min = 1.7 Kbyte/s = 14 Kbit/s
Cisco (2022 forecast): 587 Exabyte mobile traffic per year = 149 Terabit/s (82% is video!)

68

Blockchain challenges: scalability

solutions

separate applications

sharding – changes trust assumptions

trusted verification – e.g. Simplified Payment Verification

payment channels – e.g. Lightning network

69

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

70

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

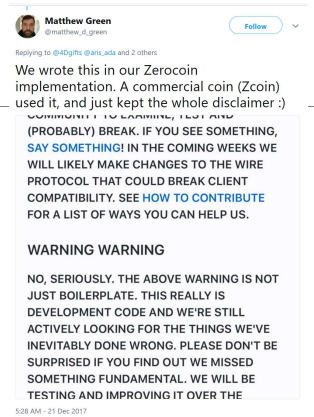
Privacy for transaction logging: Opacity

Restricted access in permissioned ledgers

71

Adding privacy

Monero:	$ 1132 M
Dash:	$ 1032 M
Zcash:	$ 375 M
Verge:	$ 108 M
Zcoin (!):	$ 49 M
PIVX:	$ 35 M

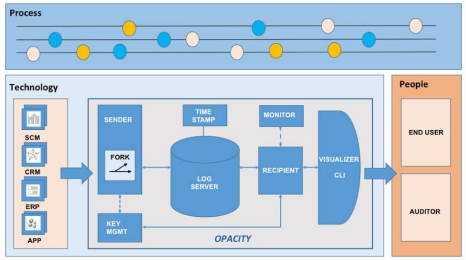


72

Distributed logging + privacy

OPACITY

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



73

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

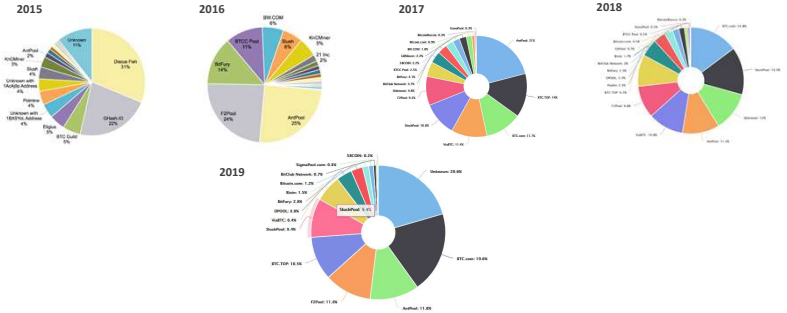
Separation of powers

Accountability

Can we learn from centuries of political science?

74

Centralization of Bitcoin mining



75

Centralization: https://arewedecentralizedyet.com/

Name	Symbol	Rank	# of client codebases that account for > 90% of nodes	Consensus	# of entities in control of >50% of voting/mining power	# of public nodes	% of money supply held by top 100 accounts	Incentivized? (/notes)
Bitcoin	BTC	1	1	PoW	4 (15% unknown)	10193	16%	Y
Ethereum	ETH	2	8	PoW	3	8610	33%	Y
Ripple	XRP	3	1	RPCA (voting system)	1	1065	78%	N
Bitcoin Cash	BCH	4	2	PoW	4 (19.44% unknown)	1554	25%	Y
Litecoin	LTC	6	11	PoW	4	214	42%	Y
Stellar	XLM	9	1	FBA	1	149	???	N
Cardano	ADA	10	1	PoS	1	1	52%	N
Monero	XMR	12	1	PoW	2 (3% unknown)	1513	???	Y
Dash	DASH	13	1	PoW	2 (15% unknown)	4720	15%	Y
Bitcoin SV	BSV	14	1	PoW	3 (4.04% unknown)	510	28%	Y
Tezos	XTZ	15	1	LPoS	??? (56% unknown)	69	18%	Y
IOTA	MIOTA	16	1	Tangle (DAG)	1	113	61%	Y
Neo	NEO	17	1	DBFT	1	52	71%	N
NEM	XEM	21	1	POI	???	442	62%	Y
Zcash	ZEC	23	1	PoW	2 (12% unknown)	389	???	Y

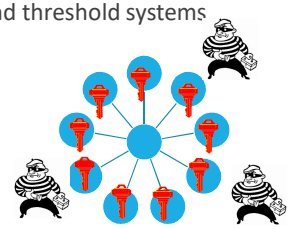
76

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



77

Blockchain challenges: cryptography crypto agility

Most blockchains have fixed crypto algorithms

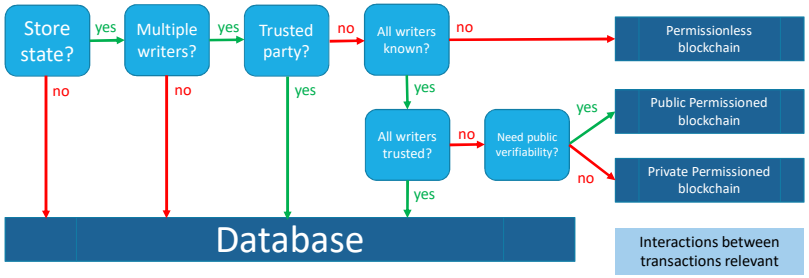
Update requires hard fork

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

78

Do you need a blockchain?

[Greenspan 2016][Wüst-Gervais 2017]



79

The death of blockchain?

MODERN CONSENSUS.

Covering the technology, people, and culture of the cryptocurrency and blockchain world

Home | Cryptocurrencies | People | Politics | Regulation | Commentary

Gartner Survey: 90% of blockchain-based supply chain projects are in trouble

The lack of well-identified use cases is causing "blockchain fatigue" to set in; caution urged for early adopters

By Leo Jakobson, May 7, 2019

only 9% invests
- technology immature
- complex, not off-the-shelf
- lack of standards
- overly ambitious scope
- misunderstanding of how blockchain could help the supply chain

80

Conclusion: blockchain

Exciting new technology for distributed consensus
- most components are 25 years old

Majority of applications only use the old components

But still strong interest in re-engineering business models

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

81

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

http://mapofcoins.com/bitcoin

S. Nakamoto. (2008) Bitcoin: A peer-to-peer electronic cash system.[Online]. Available: http://www.bitcoin.org/bitcoin.pdf

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

D. Ron, A. Shamir: Quantitative Analysis of the Full Bitcoin Transaction Graph. Financial Cryptography 2013

82

Questions?

?

83

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: @CosicBe
TELEPHONE: +32 16 321148

84