FREE LECTURE

An Introduction to Crypto Currencies, Bitcoin & The Blockchain

Lichfield. Staffs.
Thursday 16th March 6-9pm

Steve (Joe) Ratheram. (steve.ratheram@inspiring.co.uk)

inspiring co

About

Steve (Joe) Ratheram (steve.ratheram@inspiring.co.uk)

- Engineer
  - Automotive 29 years.
  - Birmingham Polytechnic / Coventry Uni / UoW.
  - Bitcoin since 2013.
  - Automotive Cyber since 2015.

- **Inspiring Company Limited** -
- *Est. 1999* www.inspiring.co.uk | @InspiringCoUK
- Automotive
  - Embedded Systems
  - Controls Calibration (Land Rover / JCB / Rolls-Royce,....)
  - Vehicle Networks e.g. Can
    - OBD Diagnostics Protocols
    - Development Protocols
  - Systems Integration
    - Safety & Validation Testing (HIL, etc.)
    - Business Development
      - Specialist Tools (Kleinknecht / Bosch / FEV)
- Automotive Cyber Security
  - Application of Blockchain / *Nakamoto Consensus Protocol* in CAVs
  - Training Automotive Penetration Testers
  - Crypto Currencies
    - Training for Police DMIs from 42 Forces, Digital Catapult,..

inspiring co

Why Bitcoin Matters

"A mysterious new technology emerges, seemingly out of nowhere, but actually the result of two decades of intense research and development by nearly anonymous researchers.

Political idealists project visions of liberation and revolution onto it; establishment elites heap contempt and scorn on it.

On the other hand, technologists – nerds – are transfixed by it. They see within it enormous potential and spend their nights and weekends tinkering with it." ...

Eventually mainstream products, companies and industries emerge to commercialize it; its effects become profound; and later, many people wonder why its powerful promise wasn't more obvious from the start.

What technology am I talking about?

Personal computers in 1975, the Internet in 1993,
and I believe Bitcoin in 2014."

- 'Why Bitcoin Matters' By Marc Andreessen New York Times January 21, 2014

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending.

We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.

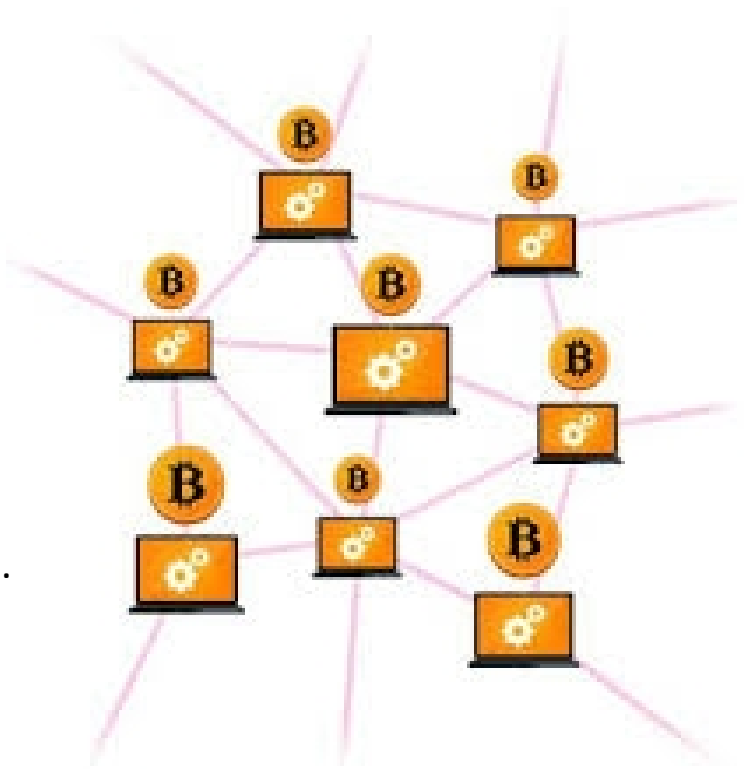
As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers.

The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Bitcoin - The Protocol

Bitcoin is an open source protocol.

- Assign any amount of value, P2P, globally ~~< 2p~~ <£1
- Users have 1..n (#public key) Bitcoin addresses.
- Private keys generate addresses and sign transactions.
- Private keys control rights of re-attribution.
- Wallets hold keys not coins.



- All transactions visible on a globally distributed public ledger known as the Blockchain.
- Blockchain replicated amongst c6500 (q1-2017) Peers.
- Size of Blockchain (1/10/14 : 23.5 MB | 1/10/15 : 45.5 MB | 2/17 ~ 126GB).
- Transactions verified by volunteer Miners via Proof-of-Work.
- Network arrives at consensus approx. every ten minutes.

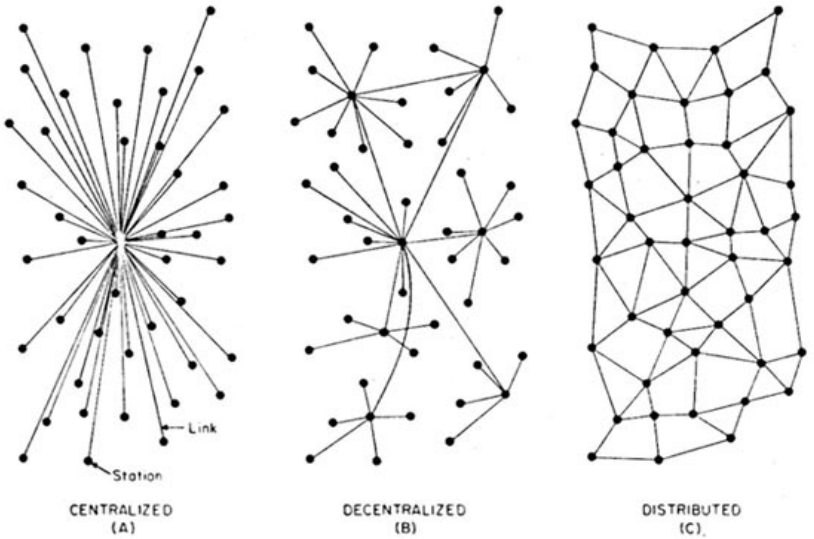
- Protocol not owned or controlled by anyone e.g. email.
- BTC transactions can contain user's custom data.
- Transactions can be scripted.

e.g. Multi Signature, ESCROW.

- New coins created algorithmically by the protocol.
- Mining Block Reward halves every 210,000 blocks approx every four years.

i.e. 12.5 [2016] / 25 [20012] / 50 [initially].

- Production difficulty algorithmically controlled VS time.
- Difficulty of mining decreases if participation falls.

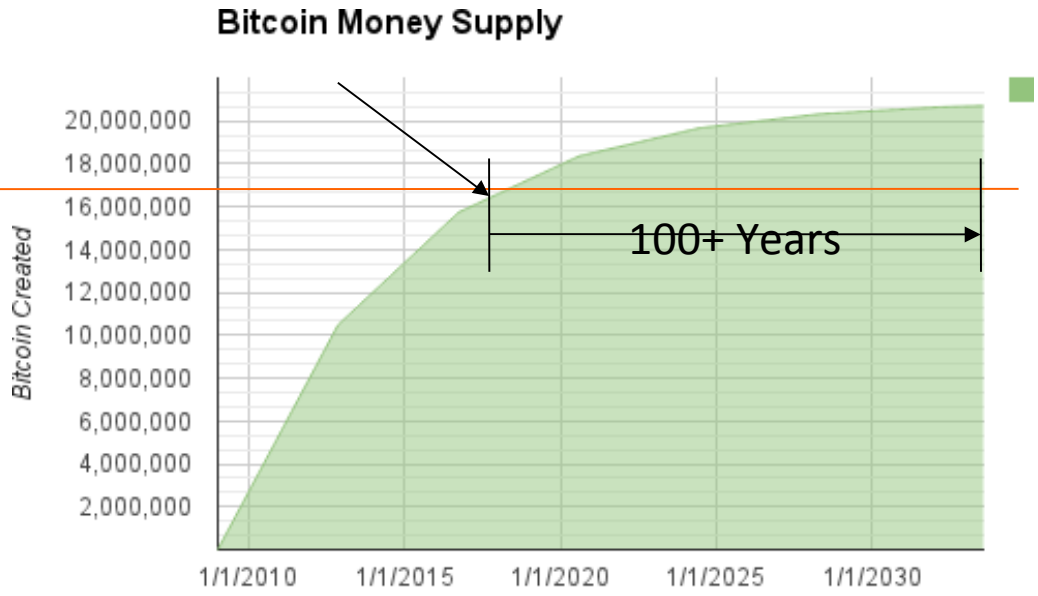


bitcoin - The Currency

bitcoin is the leading crypto-currency.

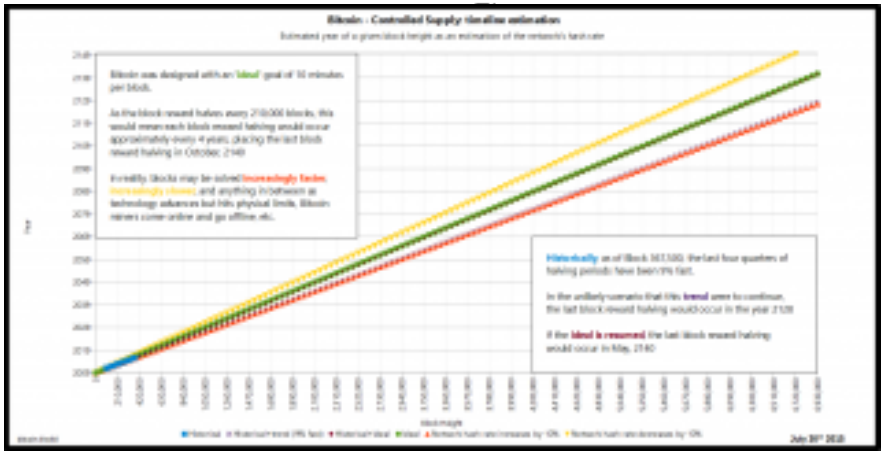
- 1 BTC = 100,000,000 *Satoshi.*
- Minimum transaction size ~~55 Satoshi.~~ 0.001 BTC

- Bitcoin has all of the attributes of *money*.
- *Durability, portability, fungibility (substitution), scarcity, divisibility, and recognisability.*
- Non reversible transaction e.g. Cash.
- Fixed issuance therefore cannot be inflated.



- Only 21,000,000 will ever be created.
  [BTC 50 in 2008 | 25 in 2012 | 12.5 in 2016] until 2140
- IF *demand >> supply (2%) THEN deflationary*

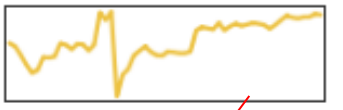
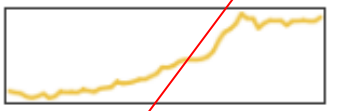
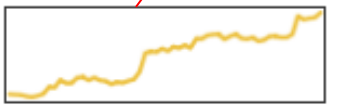
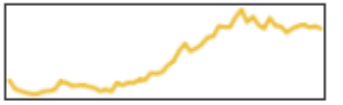
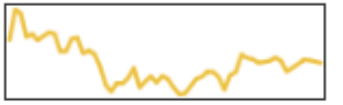
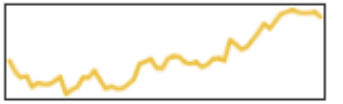
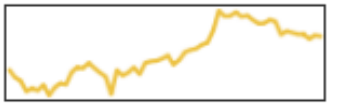
i.e. holds value & purchasing power.



- *Bitcoin described as :--*
- **Value exchange mechanism.**
- **Digital bearer instrument.**
- **Money as a digital Content Type.**
- **Programmable Money.**

- **Crucially - Embedded devices can conduct complex transactions securely according to programmatic rules.**

Crypto-currency Market Capitalisation.

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	£16,590,219,117	£1023.01	16,216,987 BTC	£194,393,724	0.52%	
2	Ethereum	~~£2,281,056,741~~ £3 BN	£25.41	£33.58 89,778,251 ETH	£79,175,919	9.52%	
3	Dash	£556,282,248	£77.63	7,166,119 DASH	£52,146,431	24.55%	
4	Monero	£211,485,444	£14.98	14,118,969 XMR	£7,499,544	5.19%	
5	Ripple	£198,372,652	£0.005320	37,290,640,853 XRP *	£958,706	2.71%	
6	Litecoin	£166,131,138	£3.31	50,196,182 LTC	£4,024,301	-0.19%	
7	Ethereum Classic	£125,144,303	£1.39	89,744,342 ETC	£3,459,223	2.57%	
8	NEM	£82,707,490	£0.009190	8,999,999,999 XEM *	£404,879	-3.44%	
9	Augur	£81,837,168	£7.44	11,000,000 REP *	£963,844	9.11%	
10	MaidSafeCoin	£64,311,536	£0.142108	452,552,412 MAID *	£306,324	-0.76%	

Distributed Smart Contracts

Privacy Centric

Clone of Bitcoin

Original pre-hard fork ETH

Distributed Storage

Total Coin Market Capitalisation :

October 2015 **c$5.1BN** , October 2016 **c$12.3BN**, Feb 2017 **c$25.6BN**

Alt-currencies & coins

- Derived or cloned from same 'open source' code.

Maybe with :-

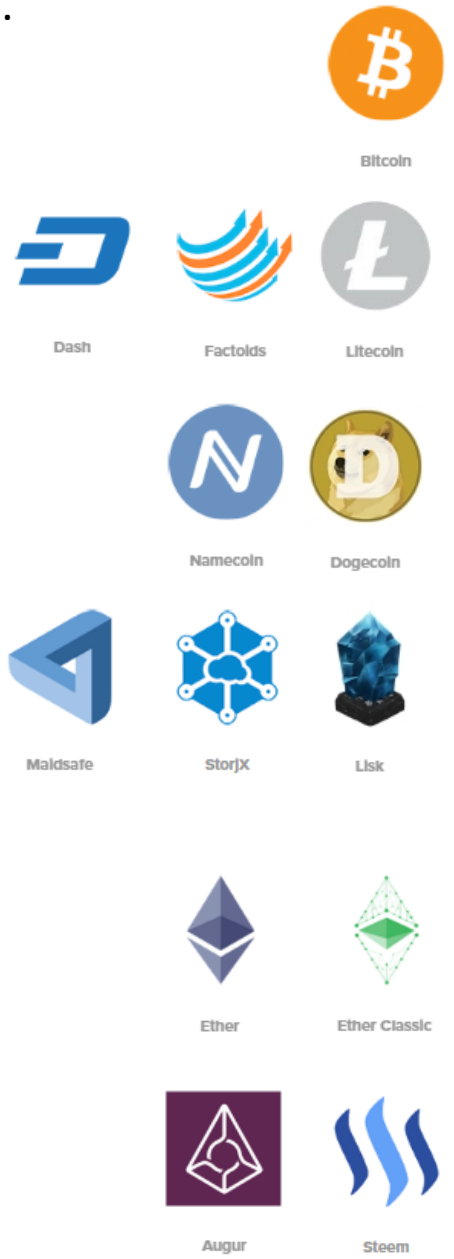
- *Different* recipe (fork). e.g. Litecoin.
- *Different* monetary policies.
- *Improved* level of privacy. e.g. Dash.

- Applications in:
  - Notarisation, Asset Transfer, Identity e.g. Factom.
  - DNS (Domain Namespace / Services) e.g. .bit e.g. Namecoin [*first-to-file paradigm*], OneName, e.g. Blockstack
  - Crowd-funding e.g., Startcoin.
  - Social Media e.g. Steem.
  - Distributed storage e.g. Maidsafe.
  - Distributed computing e.g. Ethereum. i.e. Smart Contracts.
- May use own blockchain.
- Own Proof of * (work VS stake).
- Coloured coins.

- create & track custom tokens by tinting bitcoin transactions.

- Pegging & Side-chains.

i.e. Lesser blockchain hooks into bitcoin transactional security.



Decentralisation

- Centralised systems rely on trust at the core.
  - Any central Server represent a single point of failure.

"There are only two types of Server. Those that have been hacked and those that will be hacked."

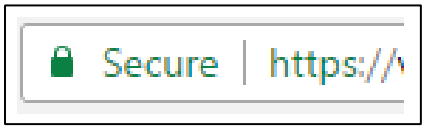
- **Examples** *US OPM (**21M** S/C a/c), Ashley Madison (**32M** a/c 30GB DATA) , T-Mobile (**15M** a/c via Experian), US IRS (300k tax a/c), Anthem (Health Ins. **80M** a/c), UCLA (Hosp. 4.5M records) Talk-talk (20k a/c), Vtech (Toymaker), Vodafone, HSBC, AT&T, Home Depot,Car-phone Warehouse (2.5M a/c), FBI (Own tools stolen),*
- ***ID, address.,DOB, DSS, Health, Tax, DVLA, Passport.***

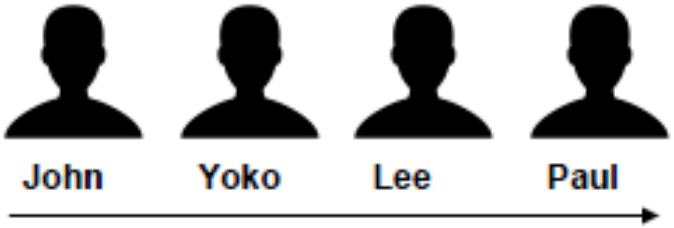
- GCHQ id 200 cyber attacks/month. (c 100 are Nat. Sec.)
- UK C/C fraud £755m in 2015 | 20,255 victims.
- 40% of C/C costs relate to fraud prevention.

- Where the incentive exists - so do the means.
- Internet overly centralised.
- Controlled by large corporations & subject to surveillance.
- Tens of billions of (IoT) devices cannot rely on centralised approaches safely.

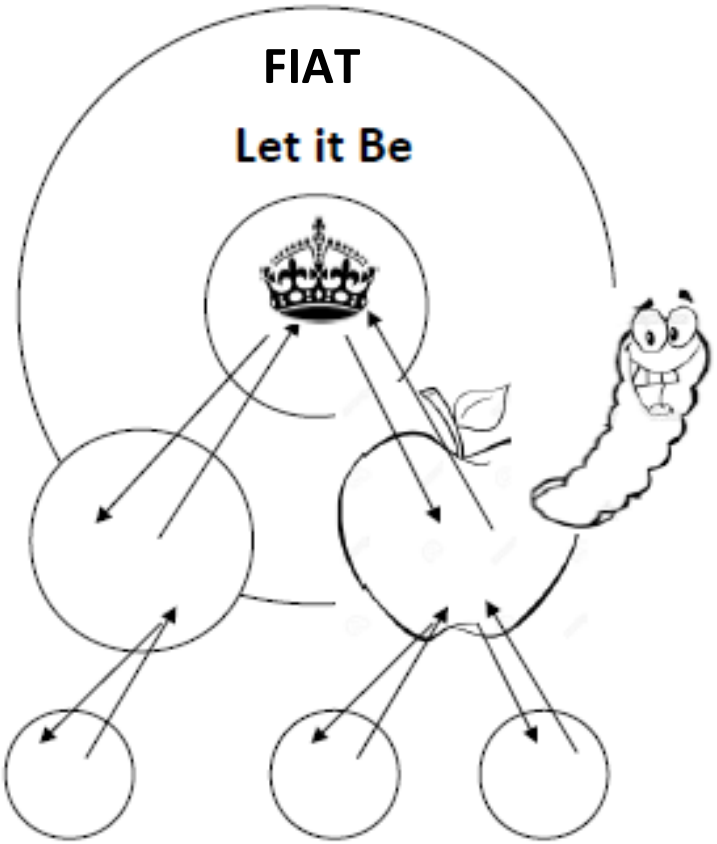
"In the near future many people will reject products and services that do no guarantee their privacy."

- Bitcoin does not need a central server or trusted third party.





Byzantine Generals Problem



Dis-intermediation

Bitcoin's Key Innovations.

Digital assets are typically easy to replicate & destrc
Bitcoin solves the "Double Spend Problem".

• Solves the “Byzantine Generals Problem”. i.e. Ensuring end-to-end message integrity without corruption.

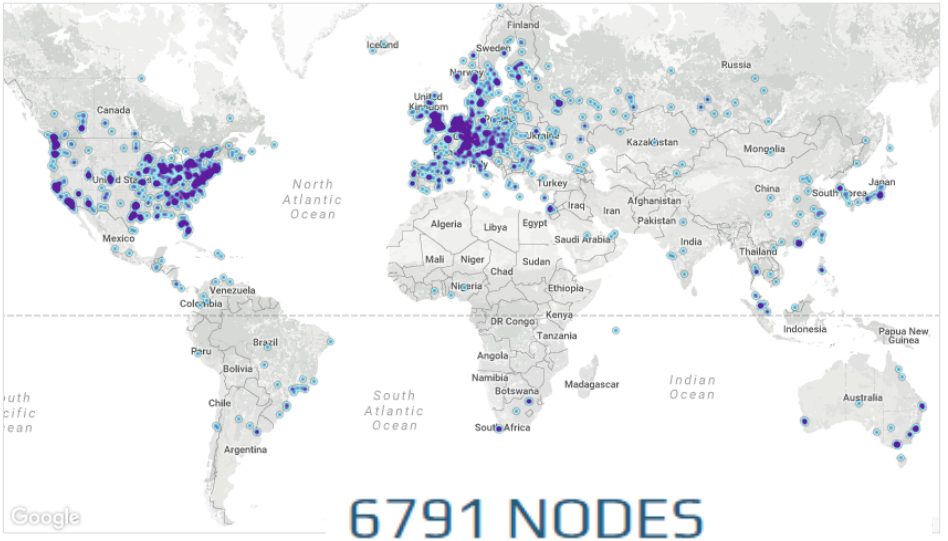
• Enables "consensus" to be reached across a P2P distributed network without the need to trust a central intermediary.

• Bitcoin is trust-less.
• Bitcoin has no central control or trusted third party.
• Principles of early internet brought to monetisation of P2P networks (DNS, Mozilla).

• No '**permission**' is required to participate.
• Net neutrality, the protocol doesn't care.

"On the Blockchain nobody knows you are a Fridge".

• High lubricity & frictionless transactions
•== Permission-less innovation.



6791 NODES

24-hour charts »

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

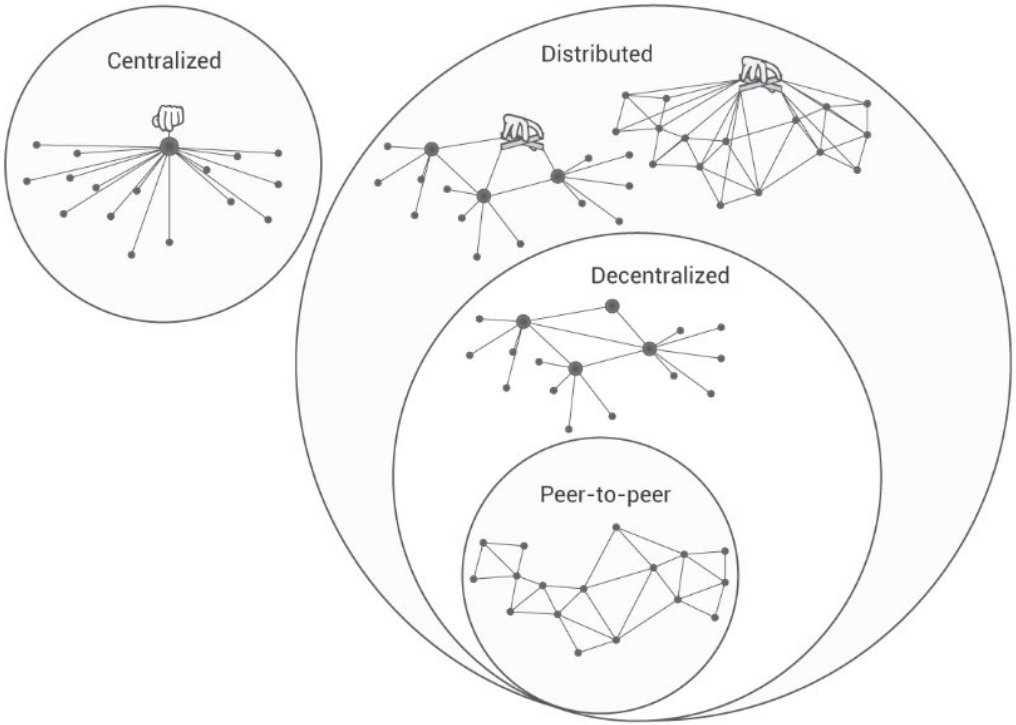
RANK	COUNTRY	NODES
1	United States	1946 (28.66%)
2	Germany	1096 (16.14%)
3	Russian Federation	430 (6.33%)
4	France	420 (6.18%)
5	Netherlands	368 (5.42%)
6	United Kingdom	285 (4.20%)
7	Canada	278 (4.09%)
8	n/a	238 (3.50%)
9	China	230 (3.39%)
10	Switzerland	108 (1.59%)

Peer-to-Peer

Peer-to-Peer Nodes (*typically*)

- Store 'own' data.
- Allow public data 'discovery'.
- Query 'other' client's data.
- Nodes are responsible for own security.
- Nodes responsible for Private Keys.
- Private Keys control rights of attribution.

- *"Not your keys - Not your currency."*
- *"Be your own Bank".*
- Security pushed to edges.

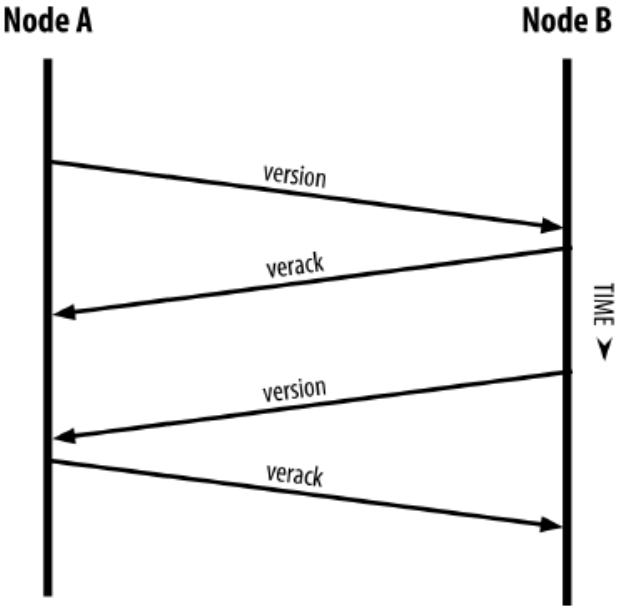


Bitcoin P2P Network

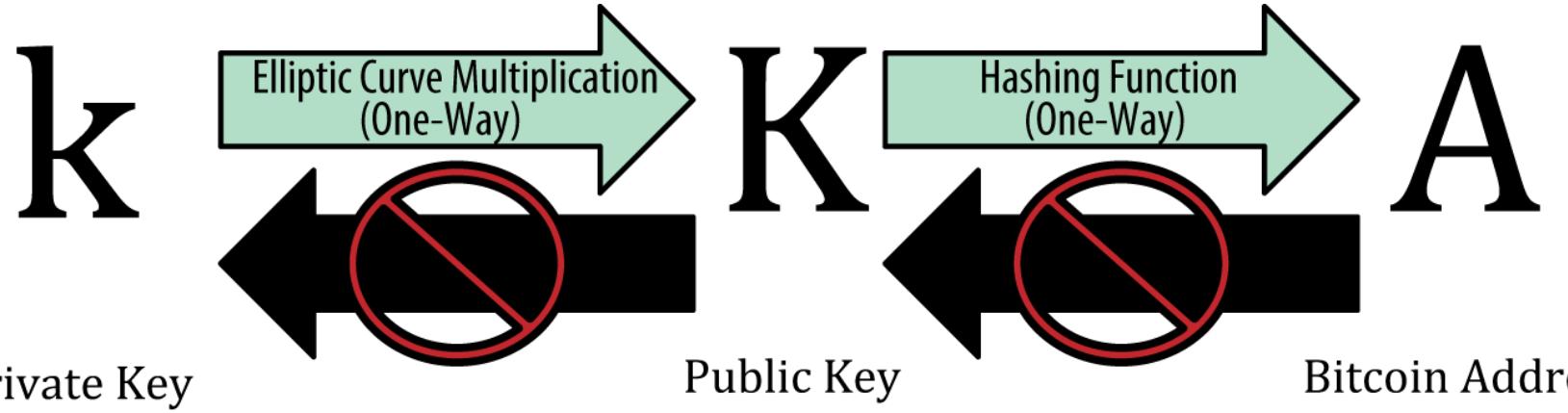
- Infrastructure: Miners, Exchanges, Wallets, Payment Processors, Users, Core Developers, Bitcoin Foundation, ..

- Consensus develops from mass participation of volunteers (peer nodes) choosing to use open source SW.

- Every peer adheres to the Bitcoin Protocol.
- Ideally has own full copy of the Bitcoin Blockchain.



Secure Hashing




```
$text = "The quick brown fox jumps over the lazy dog"
$hash = "6d12a41e72e644f017b6f0e2f7b44c6285f06dd5d2c5b075"
$text = "The quick brown fox jumps over the lazy cog"
$hash = "a8f04b0f7201a0d728101c9d26525b31764a3493fcd8458f"
```

- A hash is digital fingerprint based on agreed algorithm
e.g. SHA256 > MD5 > CRC
- By comparing the computed hash to the expected hash data integrity can be verified.
- Small changes in inputs produce very different outputs.
- Collision resistance is vital.
i.e. Any two inputs must never produce same output.
- SHA256 allows for massive integer 2^256 space.
- Collision in theory therefore improbable.

SECURE DATA

$$f_{enc}(M, K_{pub}) = E_D$$
$$f_{dec}(E_D, K_{priv}) = M$$

- Bitcoin uses pseudonymous public (addresses) & asymmetric encryption based upon [ECDSA] elliptic curve digital signature algorithm & [SHA256] secure hashing algorithm.

- These combine to instantiate transactions featuring one way mathematical trap doors that are relatively easy to verify but very hard to decompose.

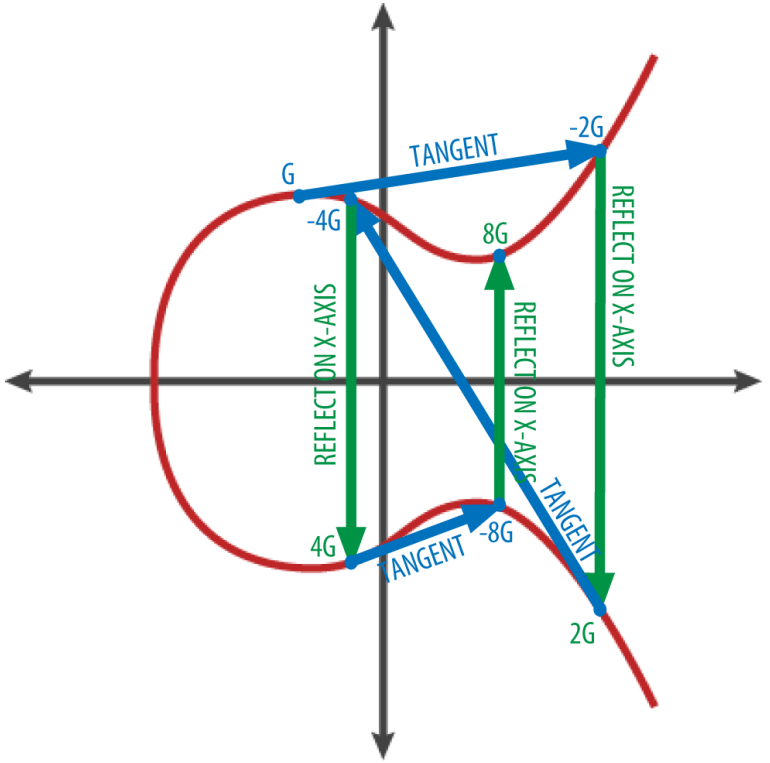
Asymmetric Keys

- Symmetric - Shared key (i.e a shared secret!).
- *Asymmetric* - Two keys, One Private, One Public.
- One to encrypt. One to decrypt.
- Keys are **mathematically related** via an Elliptic Curve Digital Signature Algorithm
- Have to be generated.
- Public key can be used to verify that the digital signature was created via corresponding Private key.

- **Private key**
- Number chosen at random (32 bytes).
- Massive space 2^256 range very hard to guess.
- Randomness (secure pseudo-RNG) is vital.
- Important to choose an [initial] *seed* with high entropy.
- Entropy is the randomness collected in HW & SW.
- Private key never disclosed.

- **Public key**
- 64 bytes uncompressed.
- Represents a point generated via ECDSA curve where y = f(x) tending towards infinity.

- Y can be implied from X and the curve formula.
- Virtually infeasible to infer i/p from o/p coordinates.



Elliptic Curve Digital Signature Algorithm

Gen expression : y^2 = x^3 + Ax + B
e.g. secp256k1 (y^2=x^3+7)

Given tangent intersects curve at two points.
Locate fixed point G. Private Key n.
Public Key P = n * G.
Symmetry means (+/-) x can be derived.
Only sign (+/-) needs to be recorded.

ECDSA (160 bits) << space << RSA (1024 bits)
- Smaller key space requires less memory.
- Fewer CPU resources.
- ECDSA >> 10 x speed >> RSA

Digital Signatures

• By signing a message the recipient can verify that the message came from the sender and was not changed in transit.

• Signatures prove both ownership of a private key, approval of a specific piece of data by the owner of that private key.

• Bitcoin's **consensus mechanism** allows users to verify that a transaction originator controls the private key.

• Bitcoin protocol verifies that the BTC value attached to a transaction is both genuine and controlled by the holder of the private key.

• *Any transfer from Node_A to Node_B must include:-*
1/ Public Key that (when hashed) yields Node_B destination address.

2/ A Signature to show Node_A controls the Private Key that generated the Public Key sent.

MESSAGING

*Alice to Bob (**M**)*

$$f_{enc}(M, K_{BOB\_pub}) = E_D$$

Bob decrypts message

$$f_{dec}(E_D, K_{BOB\_priv}) = M$$

*Bob to Alice (**M'**)*

$$f_{enc}(M', K_{ALICE\_pub}) = E_D$$

Alice decrypts message

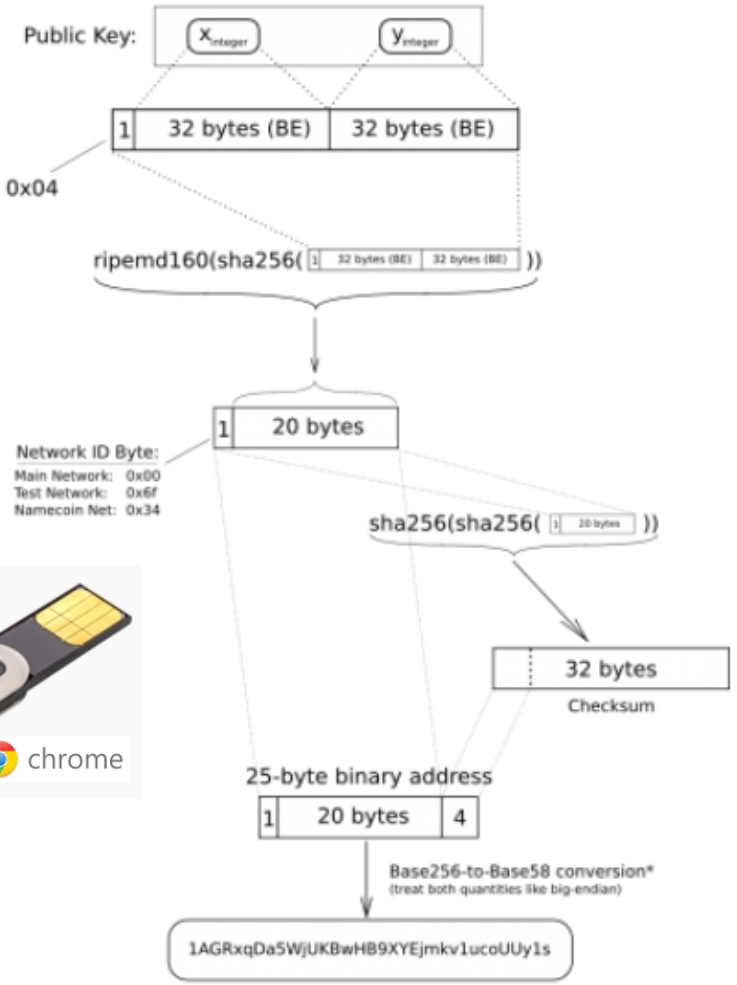
$$f_{dec}(E_D, K_{ALICE\_priv}) = M'$$

```
read EC key
Private-Key: (256 bit)
priv:
    16:26:07:83:e4:0b:16:73:16:73:62:2a:c8:a5:b0:
    45:fc:3e:a4:af:70:f7:27:f3:f9:e9:2b:dd:3a:1d:
    dc:42
pub:
    04:82:00:6e:93:98:a6:98:6e:da:61:fe:91:67:4c:
    3a:10:8c:39:94:75:bf:1e:73:8f:19:df:c2:db:11:
    db:1d:28:13:0c:6b:3b:28:ae:f9:a9:c7:e7:14:3d:
    ac:6c:f1:2c:09:b8:44:4d:b6:16:79:ab:b1:d8:6f:
    85:c0:38:a5:8c
ASN1 OID: secp256k1
```

Bitcoin Address Generation

- A Bitcoin address is derived from public portion of ECDSA key-pair.
- Bitcoin uses pseudonymous public (addresses).
- Wallets store keys.
- Keys allow holders to perform TX on the public ledger.
- Software not essential to store bitcoin.
- Addresses can be generated offline.
- Can be physical not digital. e.g. Paper wallets like a printed note.
- Money as a Content Type.
- Pseudonyms are as good as money.
- Pseudonymous NOT anonymous.
- Bitcoin addresses can be associated with IP data.

https://www.bitaddress.org



Paper Wallet

BIP39 mnemonic phrases (seeds for backup)
- 24 English / Jap etc. WORDS + PIN with Wallet

Public Address : 17Kjiz1vJiVnLVye7p7SeJ2YyuES7zHz9F

Private Key : 5KhP5uD8bbzG5VSGbcvQNrtA7W62D6fQTSy2VWtrBP3dnwrWg5g

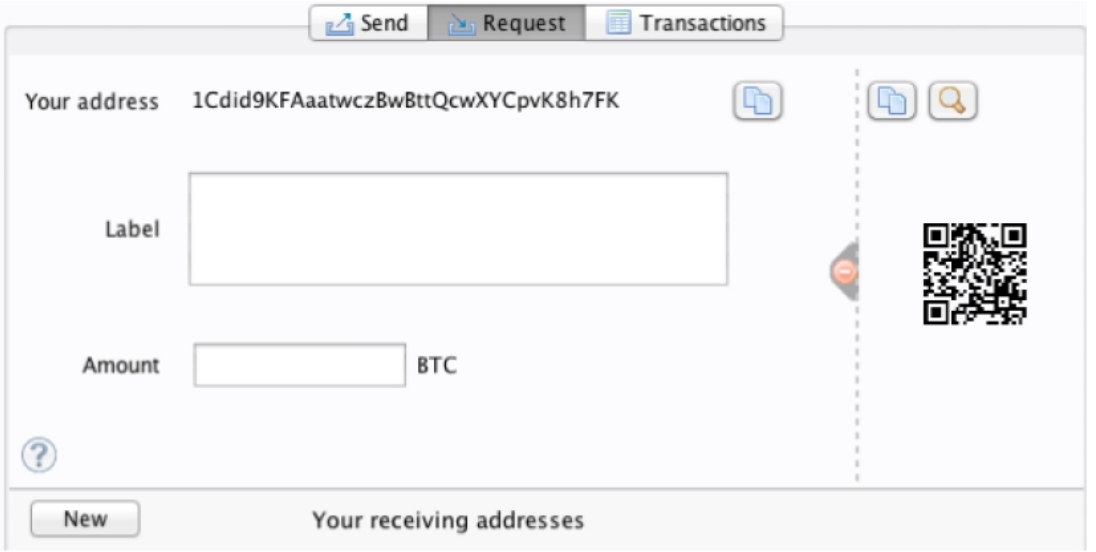
Transactions

- If a Bitcoin transaction is structured properly and signed with a private key the network will route it.

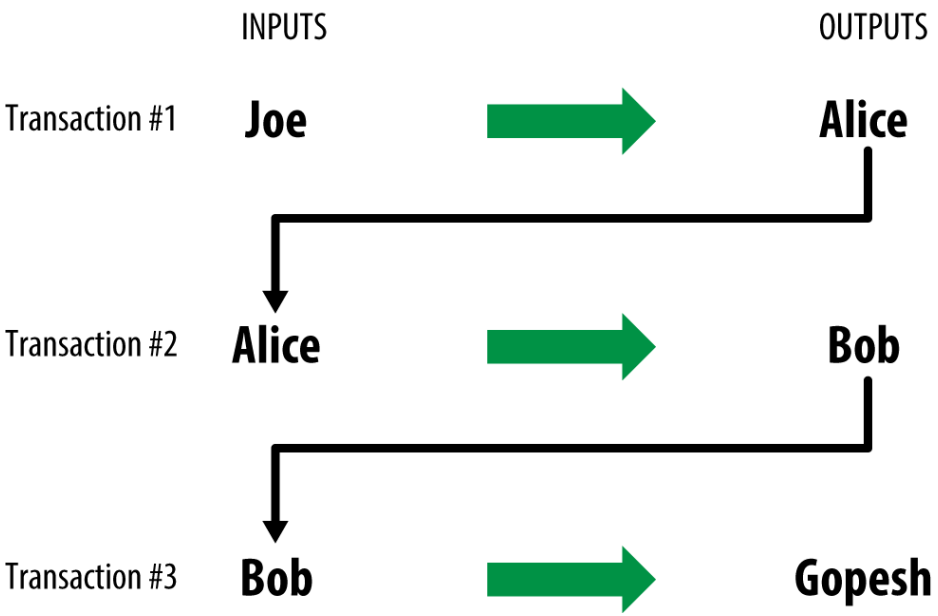
- c33 character. transaction may be encoded by many means.

- Not essential to be online in areas with little connectivity or electricity.

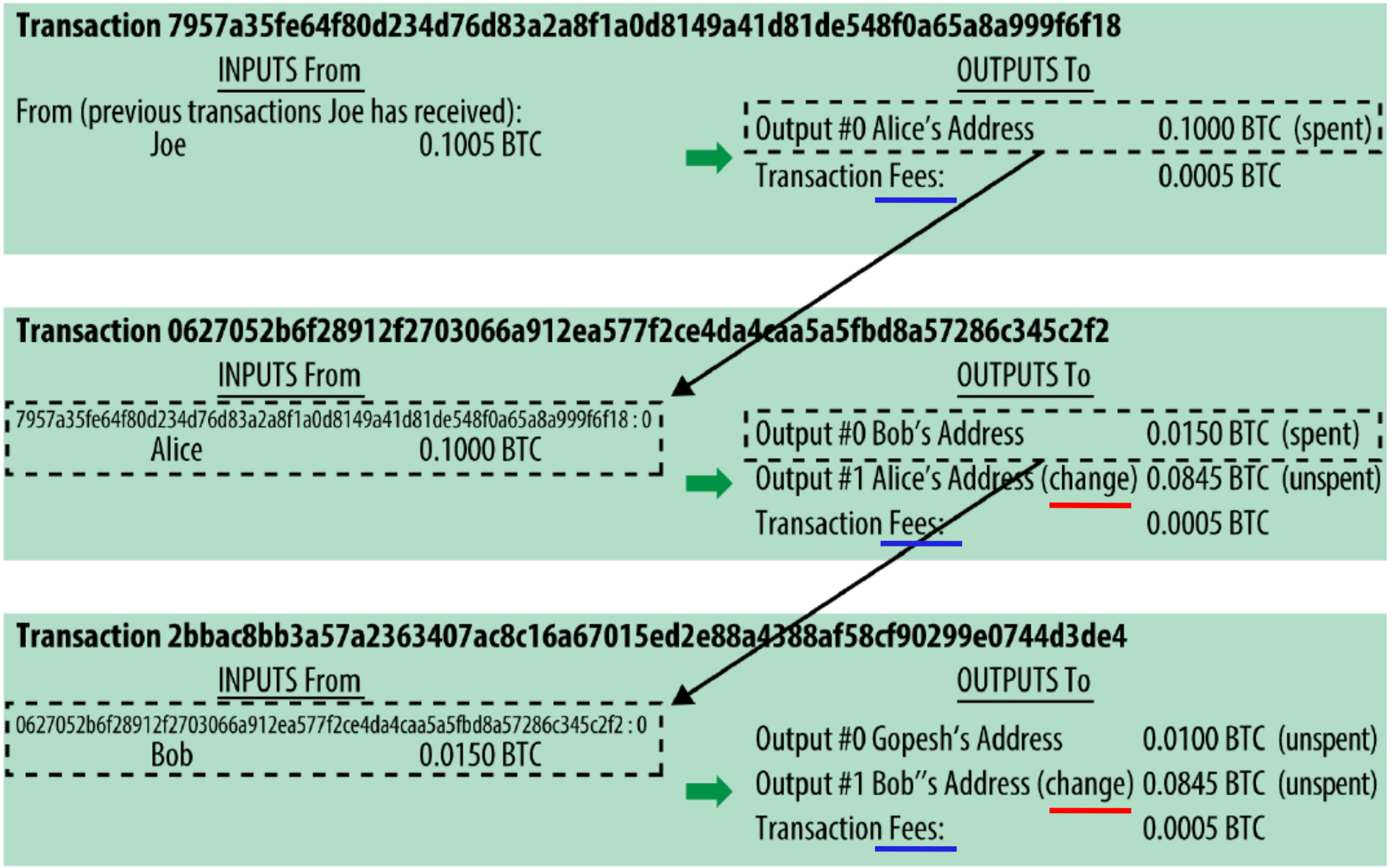
- Transaction only has to reach a miner e.g. via SMS, Radio, etc.



https://bitcoin.org/en/**choose-your-wallet**



Transactions



An Unspent Transaction Output (**UTXO**) that can be spent as an input in a new transaction.

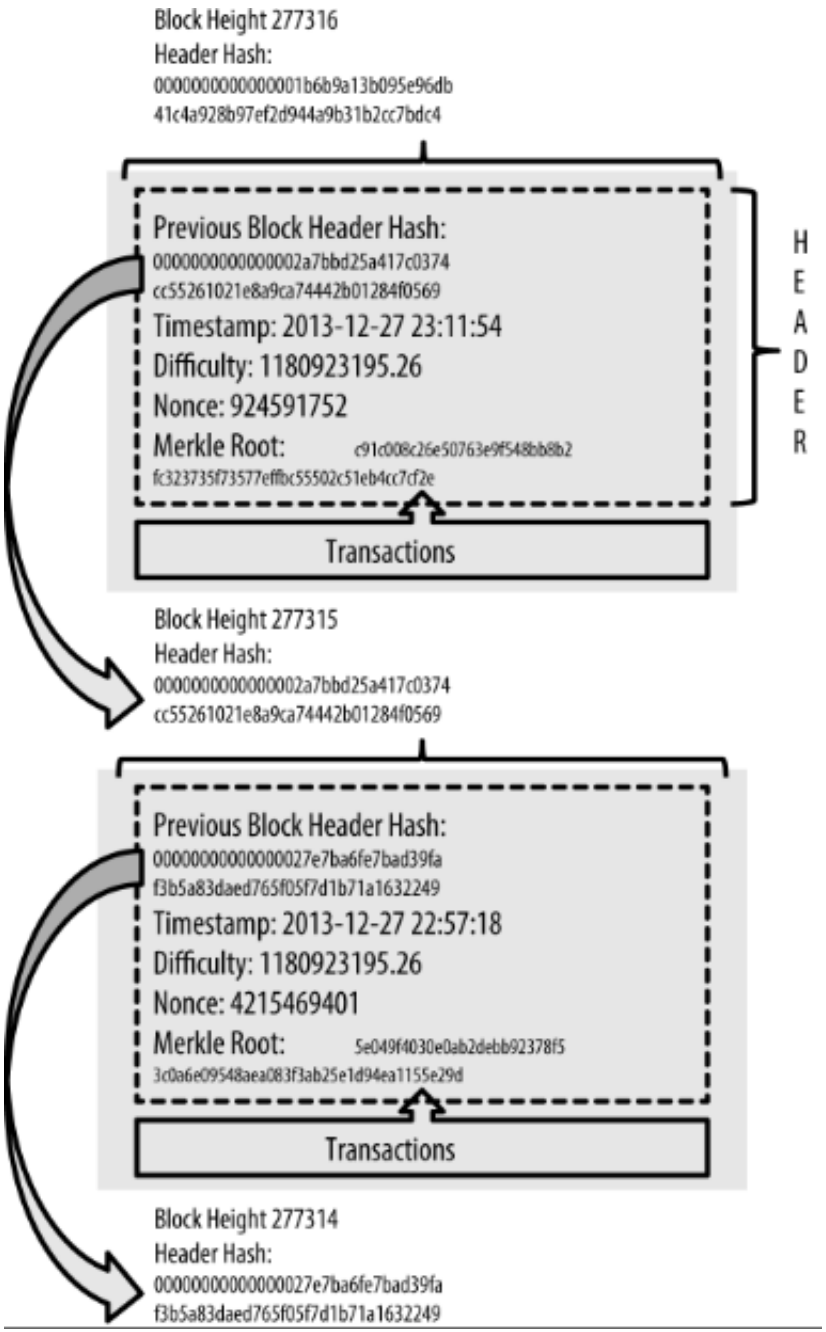
Blocks

• Transactions propagated instantly into a mem_pool.

• Each block contains
  - **Ref**erence / # of the previous block header.
  - **Time**-stamp
  - N**once (**random number issued once).
    ** **Important key to puzzle** **
  - **Merkle Root**
    + (root hash of a data structure called the Merkle tree storing all transactions in the block.
  - **Transactions** that have taken place since the previous block.

• Changing any part of any transaction retroactively would alter the transaction ID, in turn altering the block header.
• Altered block header would no longer meet the proof of work requirement.
• Double spending transactions are detected & ultimately invalidated & ignored.

• Promises to pay the bearer are verified & stored by everybody who "mines" the network.



Bitcoin Blockchain

- Ongoing "chain of hash-based proof-of-work".
- Represented in the form of an immutable shared ledger (blockchain) constructed on a longest chain wins basis.

- **Blockchain ==** distributed, public, time-stamped, Immutable, Tamper-proof ledger.

- Consensus reached every 10 minutes.
- *1 block mined = 1 confirmation (Max 10 minutes), 2 bocks = 2 confirmations. Max 6 confirmations.*
- Task likened to Sudoku puzzle.
- "hard to solve / easy to verify."
- More network participants solve the problem sooner.

- The network calibrates the 'proof of work' computation to always be c10 minutes hard irrespective of the amount of participating peers.
- e.g. compare A (block hash) target to difficulty X.

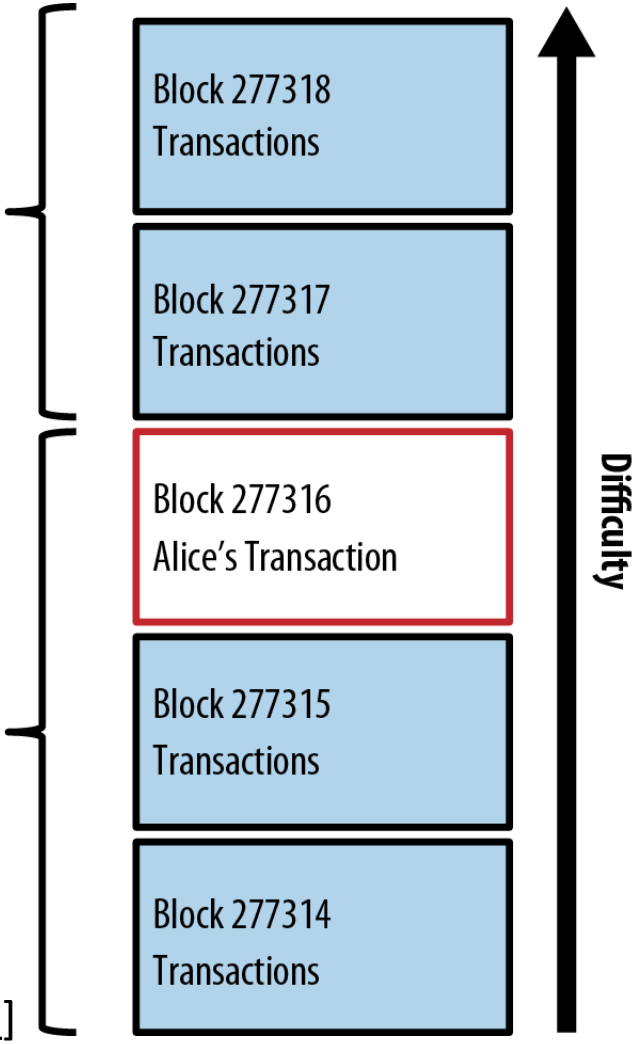
If X reduces it's harder to find A ~ in smaller range.

- Difficulty calculation performed every 2016 blocks c2 weeks [2016]
- IE Hash must be below difficulty target to be valid [*limbo competition*]

https://youtu.be/OeJQ0aJFa9Y?t=1680

Mining Block Reward halves every four years.

- Production difficulty algorithmically controlled VS time.
- Difficulty of mining decreases if participation falls.



Proof of Work / Mining

• The protocol rewards miners for risking energy and computing power to validate transactions by conducting **proof-of-work**.

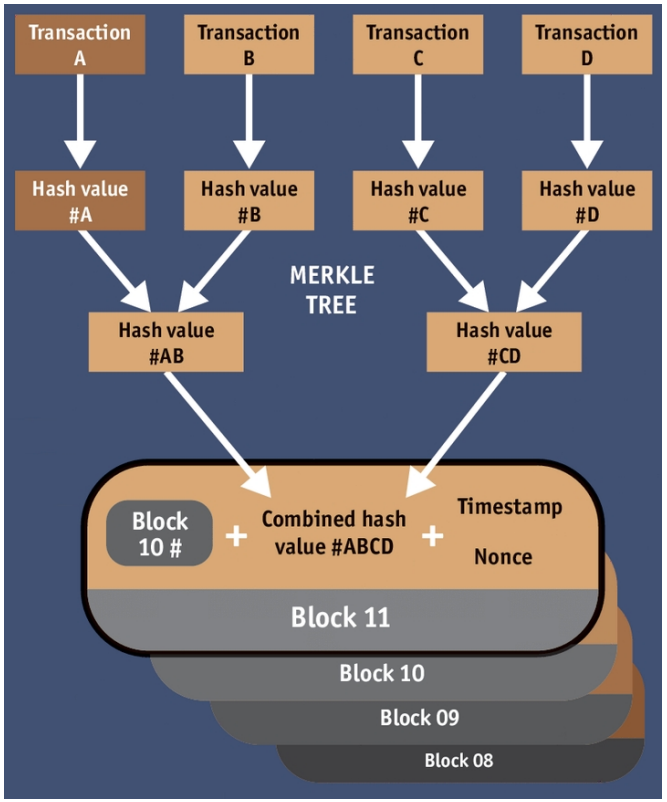
• Real world resources are expended on solving *computationally expensive task*.
• The Bitcoin Formula: *Energy / Time = Truth.*

• The protocol derives consensus about transactions assembled into blocks by validating cryptographic inputs to confirm entitlement.

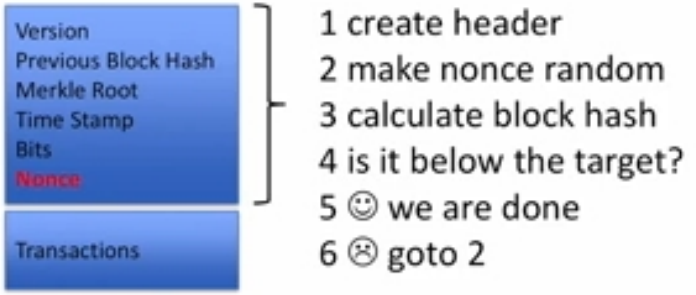
• The block header becomes part of a cryptographic puzzle solved by manipulating the Nonce.

• Once a solution is found the new block is added to the Blockchain.
• New coins created algorithmically by the protocol.

• Solving the problem actually comes down to guesswork.
• Winning the coins then employs game theory & requires luck.



Block hash must be below the target difficulty

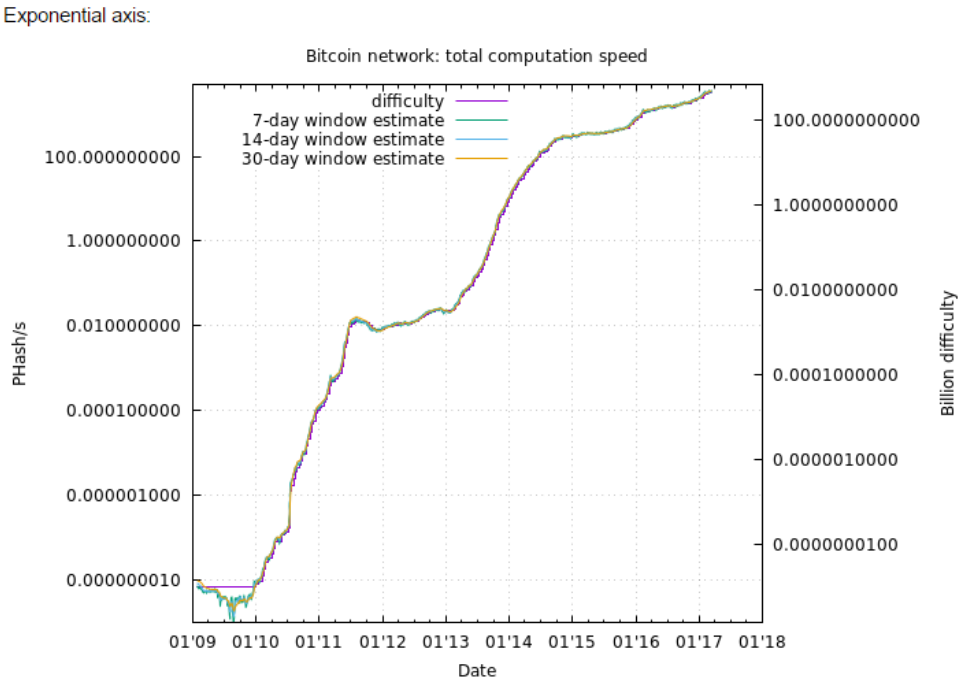


Block# 321511 ~ 250,000,000 GH/s

0000000000000001fb68313c9728ec3728686a632ad36c31fe9a9bf4b112362

Bitcoin Security

- Security relies on widespread participation and the majority of peers being “good actors”.
- If there are more good than bad the longest (correct) chain eventually wins.
- To change history attackers must marshal >51% of network hashing power.
- Economics of rewriting VERY punitive.
- CPU power & energy costs c $400M to fool network for 10 minutes.
- Bad actors capable of subverting the network must suspend self-interest since such hashing power earns more by mining legitimately.

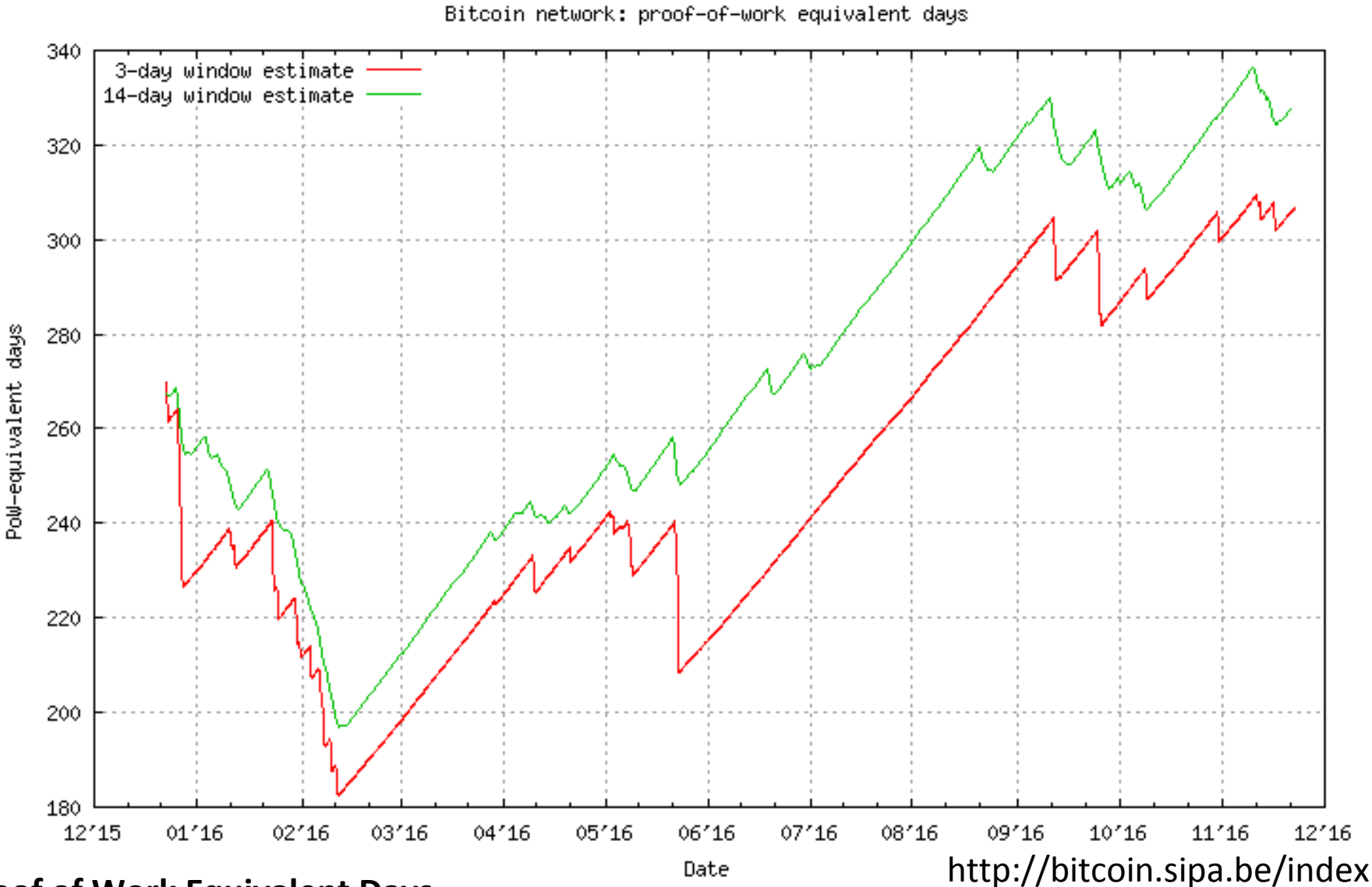


- A chain of trust. | A 'trust machine'.
- Bitcoin is an information network backed by Energy / Time == Truth
- Problem of new technology running on old infrastructure. Weak points e.g. exchanges get hacked.
- Bitcoin protocol never been hacked.

- Mt. Gox. Bitcoin exchange.
- Bitstamp. Exchange. ...
- Bter. Exchange. ...
- Picostocks. Exchange. ...
- Inputs.io. Wallet.
- Shapeshift
- Blockchain.info
- The DAO
- ....

“ How did we end up with, within four years, the most powerful payment processing system on the planet - built by Geeks in their garages without anyone noticing ? “
(A. Antonopoulos)

Bitcoin Immutability

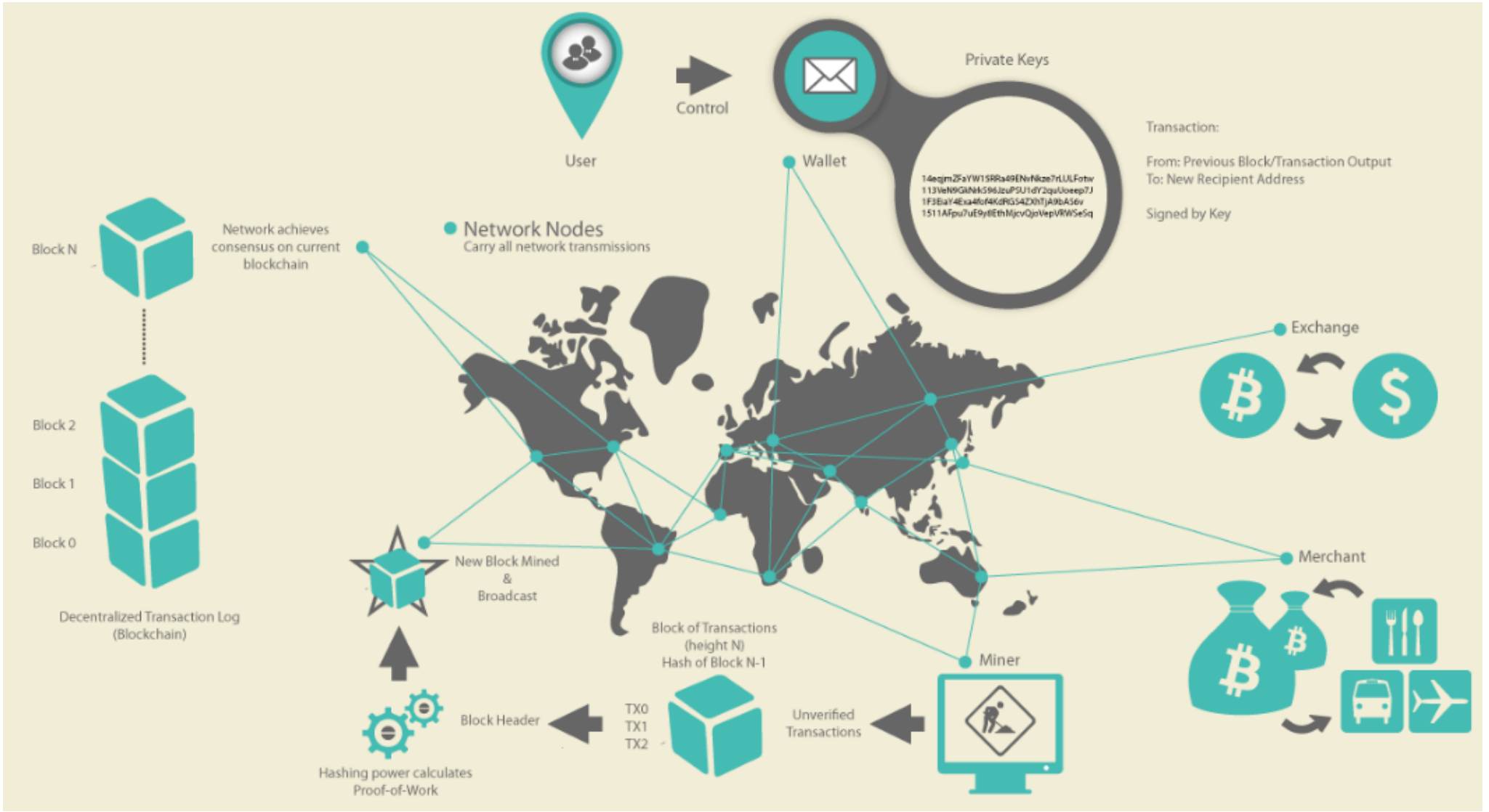


http://bitcoin.sipa.be/index.html

Proof of Work Equivalent Days

The ratio of total work divided by estimate of hash-rate at that time. Thus it's the amount of time it would take for an attacker with 100% of the hash-rate to rewrite the entire blockchain.

Network Overview



Satoshi Nakamoto's Motives ?

```
GetHash()      = 0x000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
hashMerkleRoot = 0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
txNew.vin[0].scriptSig     = 486604799 4 0x736B6E616220726F662074756F6C69616220646E6F63657320666F206B6E697262206E6F20726F6C6C65636E6168432039303032 2F6E614A2F33302073656D695420656854
txNew.vout[0].nValue       = 5000000000
txNew.vout[0].scriptPubKey = 0x5F1DF16B2B704C8A578D0BBAF74D385CDE12C11EE50455F3C438EF4C3FBCF649B6DE611FEAE06279A60939E028A8D65C10B73071A6F1671927485 5FEB0FD8A6704 OP_CHECKSIG
block.nVersion = 1
block.nTime    = 1231006505
block.nBits    = 0x1d00ffff
block.nNonce   = 2083236893

CBlock(hash=000000000019d6, ver=1, hashPrevBlock=0000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505, nBits=1d00ffff, nNonce=2083236893, vtx=1)
  CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
    CTxIn(COutPoint(000000, -1), coinbase 04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f7220 6f6e20627269 6b206f66207365636f6e6420626169 6c6f757420666f722062616e6b73)
    CTxOut(nValue=50.00000000, scriptPubKey=0x5F1DF16B2B704C8A578D0B)
  vMerkleTree: 4a5e1e
```

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Implications

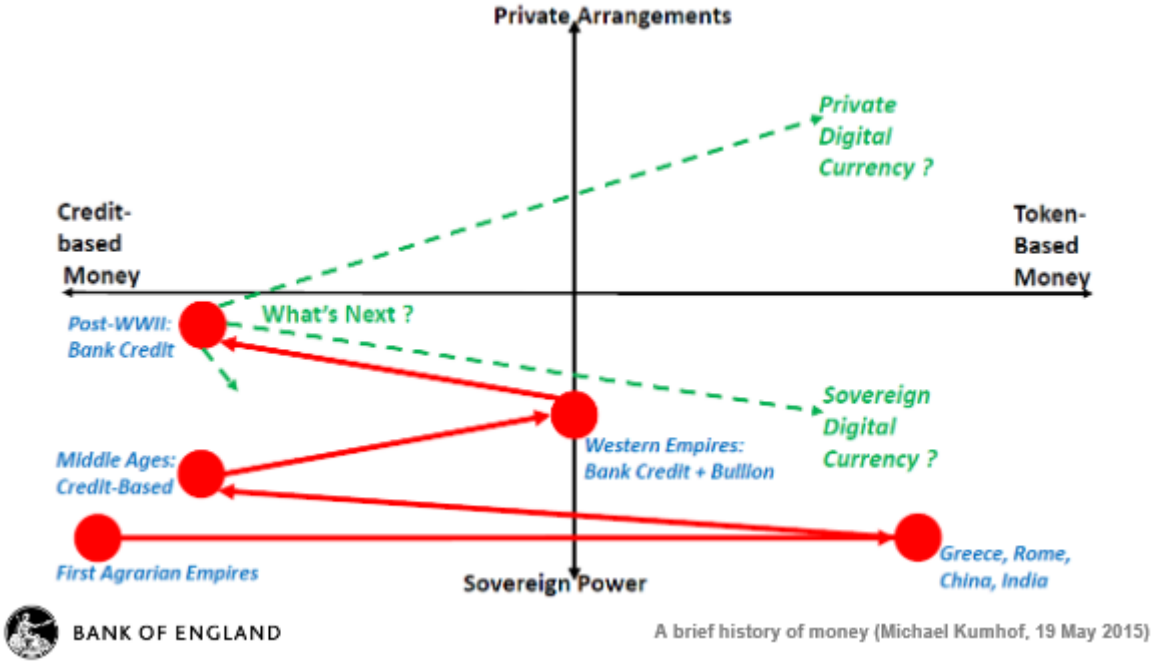
- **Political**
  - Border-less Payments.
    - Criminal use (VS Cash, Pay Pal).
    - Terrorist use (VS CA$H].
  - "Ability to apply economic sanctions!" [EBA].
  - Benefits to business / trade.
  - Control VS Regulation.
  - *"Risk of trying to regulate a de-centralised system with centralised thinking".*
  - Privacy.
  - "*How much are you prepared to fight for ?.*" [BoE].
- **Economic**
  - Frictionless Payments / Innovation
    BoE planning "BritCoin".
    UK Gov't estimates "20% of notes/coins issued as as crypto-currency may increase GDP by 3% permanently".
  - Vast potential for economic inclusion / trade.
    2/3 of the world's 6BN people unbanked.
  - International Remittances
    African migrants send home $550BN.
    One foreign worker supports up to 12 people.
    Moneygram/Western Union (Mkt Share 80%)
    charge for $300 typically 10+% = $175BN profit.
    Bitcoin savings amount to $100BN retained in economy.

Implications

- **Social**
  - Incentives & rewards e.g. Hull Coin
  - Employment, sector creating jobs.
  - Social security rewards built-in.
  - Distributed people / systems are less vulnerable to attack.
  - Energy efficiency VS planetary scale immutability.

- **Technological**
  - Bitcoin appears to be just a currency - in fact it is just first application.
  - A key platform for innovation, more modes of work than currency.

  - A data layer for the blockchain. *e.g. notarisation of assets, smart contracts, transfer of ownership, proof-of- existence.*
  - IoT / Connected Cars. *nb. K**ey challenges are Secure Random Number and Pseudonym generation / management.***



Summary

- Bitcoin and the Blockchain may well prove to be the most important **disruptive** computer science innovation since the birth of the Internet.

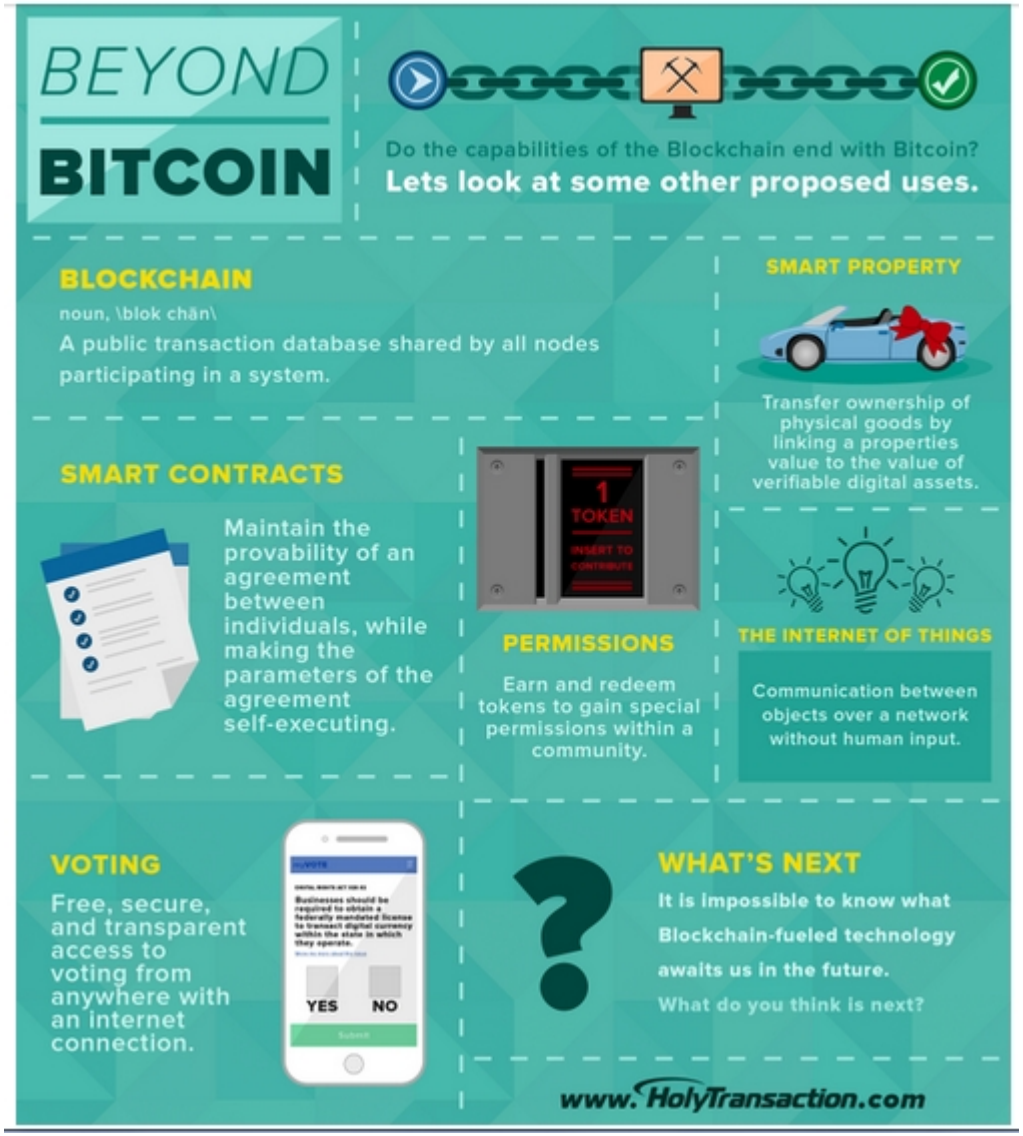
- First distributed proof of work & decentralised ledger that many thought impossible.

- New design paradigm for secure network communications.

- May help monetise the IoT, connected cars.
- May enable secure driver-less cars at scale.

- Largest public cryptographic PKI deployment in the world.
- `[Jan 16] bitcoin network c300,000 times more powerful than the world's fastest supercomputer.`

- Bitcoin is the internet of money.
- Bitcoin the *de facto* money of the internet.



" Banks brought you the recession and Geeks brought you the internet.
-- Who are you going to trust ? "

Thank you for supporting this Event

inspiring co

Join us at ....

coinfest UK

HOME EVENTS PARTNERSHIPS CONTACTS & NEWS BOOK TICKETS (LIVE)

Join us in Manchester at The Manchester Conference Centre on April 7th & 8th 2017

Our aim is to bring people together from all over the UK for two days packed full of speaker presentations, activities and raffles! Topped off with free food and crypto goodie bags!