

Cryptocurrency



Bitcoin & Cryptocurrency Technology



Roadmap

Cryptography

Identities

Blockchain

Bitcoin & Mining

Altcoins

BITCOIN OWNERS



What my friends think I do



What my mom thinks I do



What society thinks I do



What Politicians think I do



What I think I do

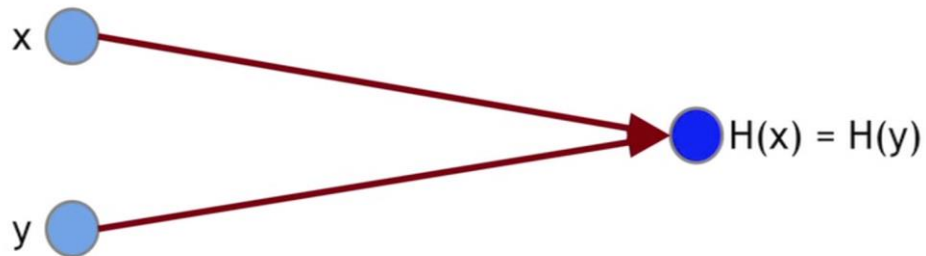


What I really do

Cryptography

Hash function $H(x) = y$

Collision-Free



Puzzle

$$H(\text{puzzleId} \mid x) = \text{hash}$$

Identities Addresses

Signatures - API

`generateKeys(size)`

`pk: publicKey`

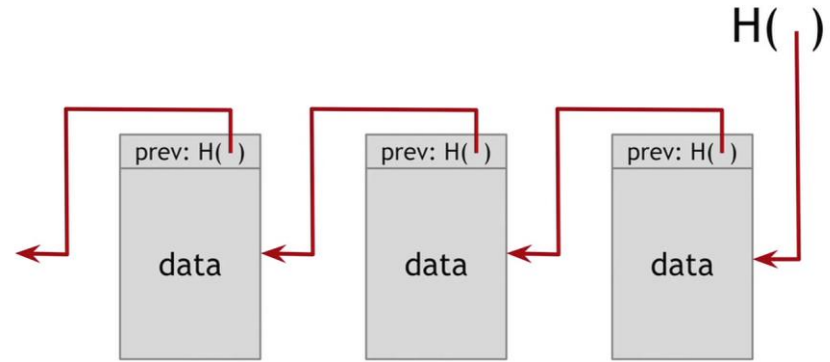
`sk: secretKey`

`sign(sk, hash(msg))`

`verify(pk, hash(msg), sig)`

Blockchain

Hash pointer structure



Data cannot be changed

Append only ledger

Bitcoin Block PoW

Header

Hash previous block

Hash this block

Difficult target (nonce)

Transaction list

Signatures

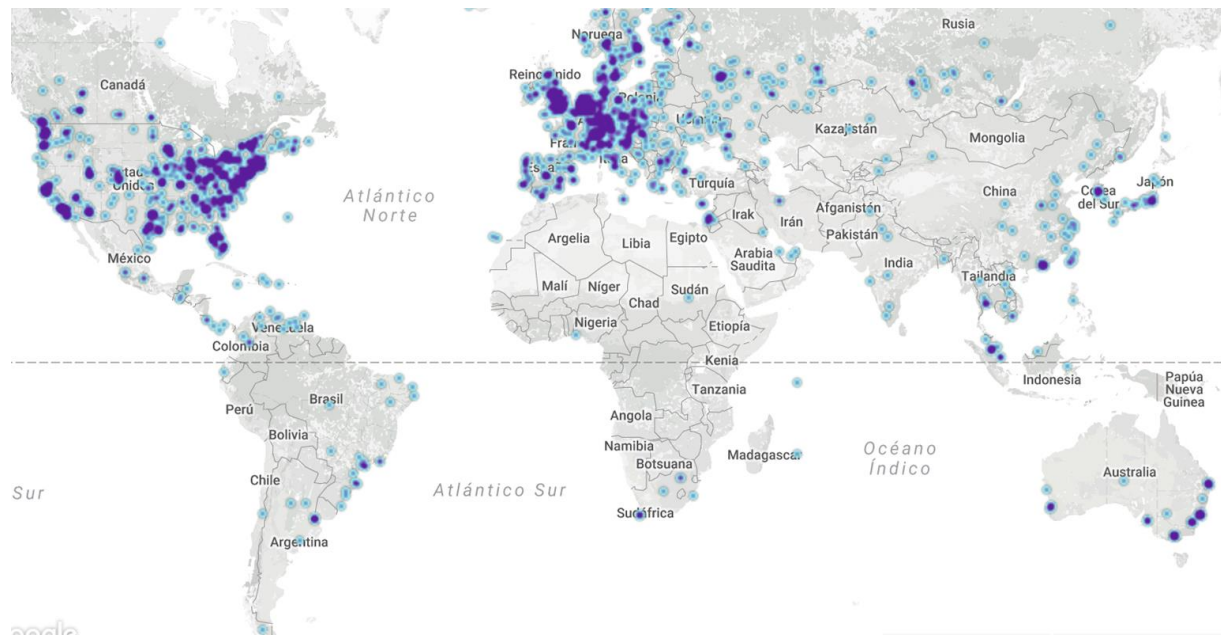
Bitcoin Decentralization

Identities

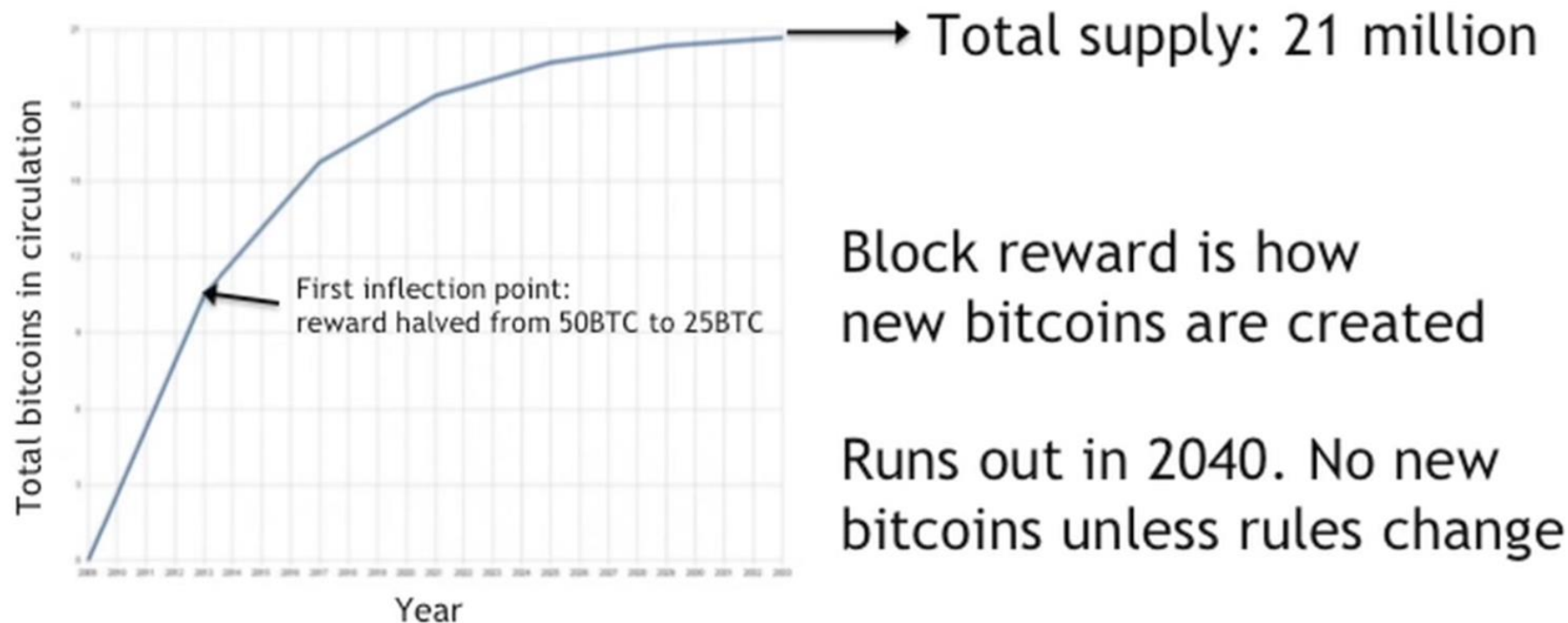
Nodes

Consensus Protocol

Peer-to-peer



Bitcoin

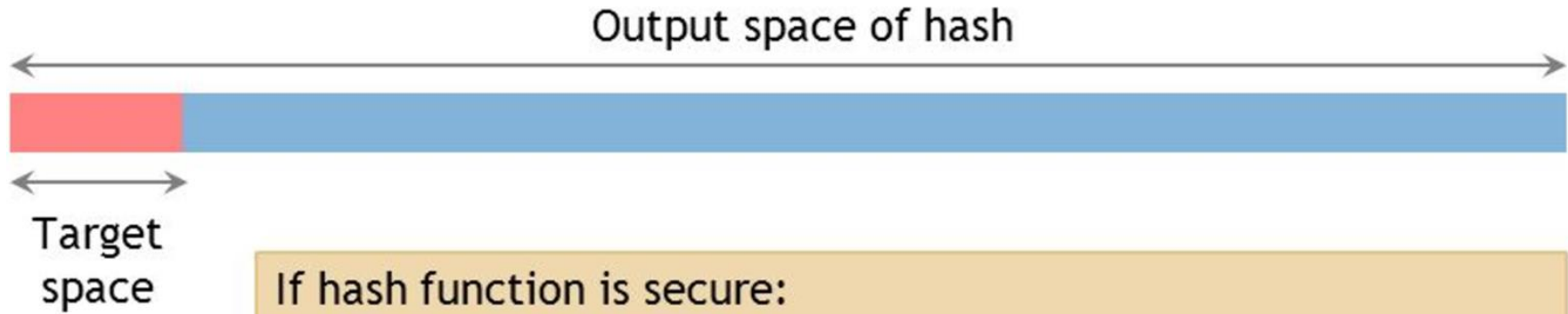
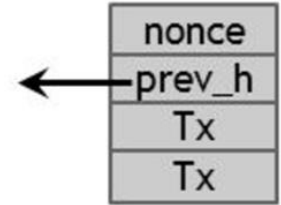


Block reward is how new bitcoins are created

Runs out in 2040. No new bitcoins unless rules change











Hash Puzzle PoW

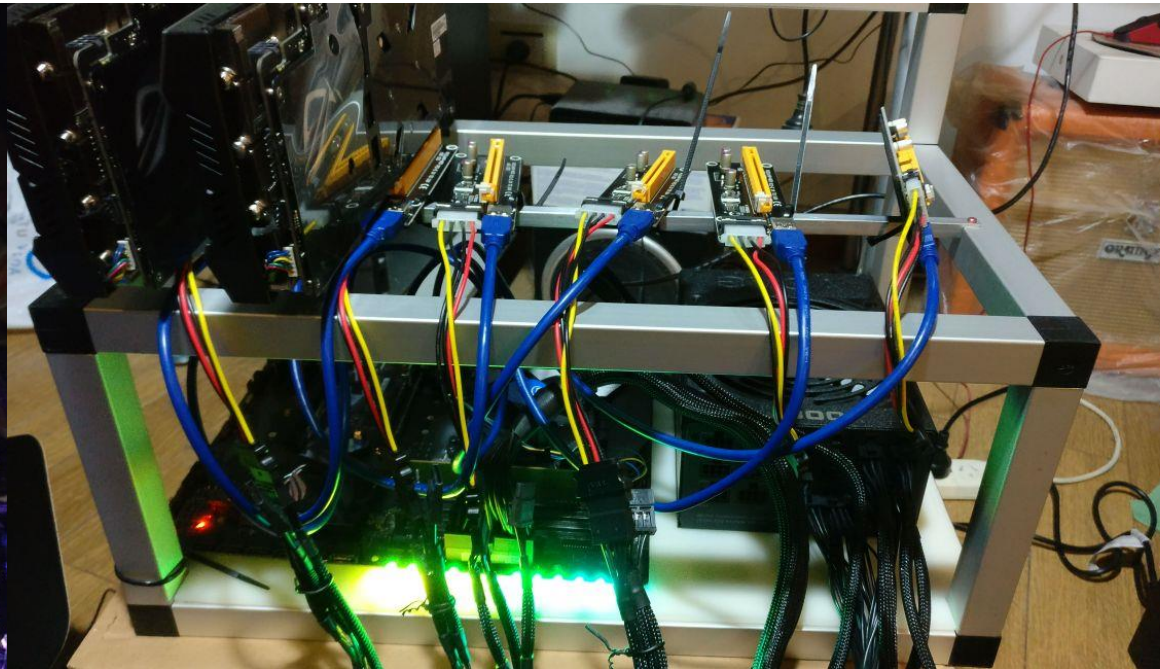
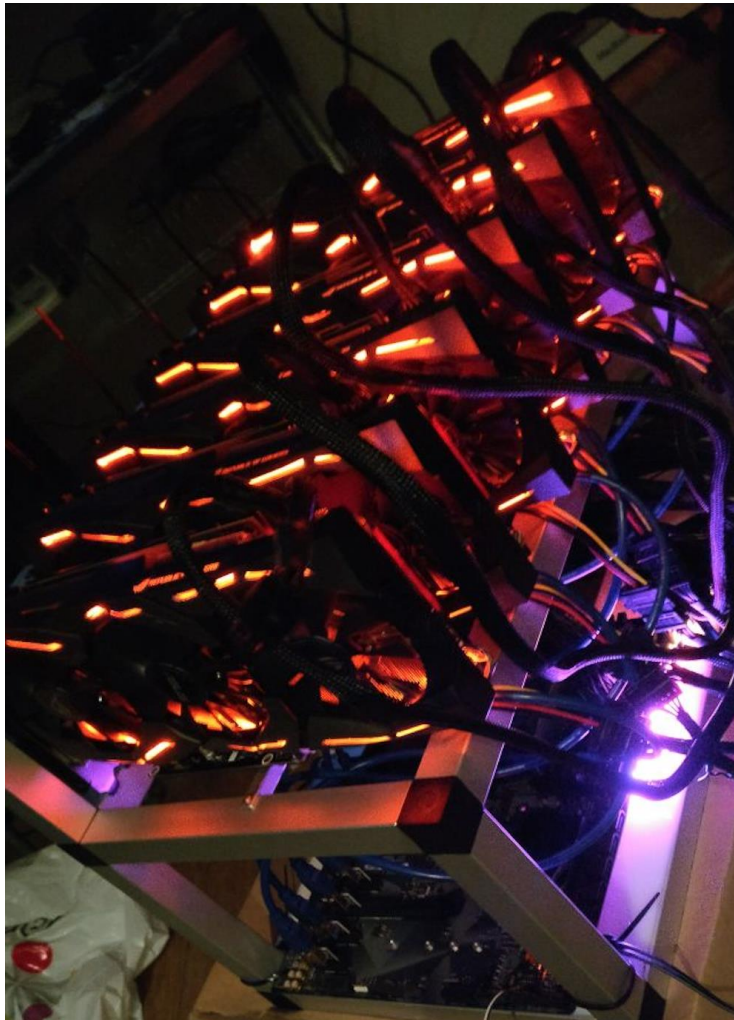
To create block, find nonce s.t.
 $H(\text{nonce} \parallel \text{prev_hash} \parallel \text{tx} \parallel \dots \parallel \text{tx})$ is very small



If hash function is secure:
only way to succeed is to try enough nonces until you get lucky

Altcoins Market

#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)
1	 Bitcoin	\$45,711,864,237	\$2774.46	16,475,950 BTC	\$1,316,000,000	2.57%
2	 Ethereum	\$17,574,111,696	\$187.69	93,632,716 ETH	\$668,716,000	-7.54%
3	 Ripple	\$6,197,809,099	\$0.161683	38,333,090,674 XRP *	\$86,847,600	-6.06%
4	 Litecoin	\$2,081,937,185	\$39.87	52,215,257 LTC	\$150,973,000	-5.50%
5	 NEM	\$1,442,421,000	\$0.160269	8,999,999,999 XEM *	\$4,041,850	-6.19%
6	 Ethereum Classic	\$1,308,651,881	\$13.92	94,008,971 ETC	\$55,218,600	-4.29%
7	 Dash	\$1,304,219,453	\$174.95	7,454,642 DASH	\$38,432,000	-10.30%
8	 IOTA	\$735,319,177	\$0.264548	2,779,530,283 MIOTA *	\$2,523,980	-2.84%
9	 Monero	\$642,324,076	\$43.24	14,854,137 XMR	\$16,738,600	-2.68%
10	 Stratis	\$460,957,522	\$4.68	98,481,729 STRAT *	\$13,432,900	0.51%



Questions?

Thanks!