Blockchain pt.2

Specific Problem -> Dedicated hardware

1932: https://en.wikipedia.org/wiki/Bombe
2005: https://link.springer.com/content/pdf/10.1007/11545262_9.pdf
Asic: https://en.wikipedia.org/wiki/Application-specific_integrated_circuit
2017: https://blockchain.info/it/charts/hash-rate

Note:
Single cpu 1 GHz ~ 6 MHash/s
P(solve a block with 1 GHz) ~ 10^6 / 10^7 10^12 = 10^-13
P(6 in Superenalotto) ~ 10^-9

Memory Based Proof of work:
Zerocoin: https://zcoin.io/wp-content/uploads/2016/11/mtpwhitepaper.pdf
birthday paradox: https://en.wikipedia.org/wiki/Birthday_problem

Hashrate Distribution: https://blockchain.info/pools

Game Theory

Selfish Mining:
https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/
Paper: https://www.cs.cornell.edu/~ie53/publications/btcprocfc.pdf

Transaction Fees: https://blockchain.info/it/charts/transaction-fees?timespan=2years
Waiting Time: https://blockchain.info/charts/median-confirmation-time?timespan=2years
Rewards: https://en.bitcoin.it/wiki/Pooled_mining
nota:
https://bitcoin.stackexchange.com/questions/59896/steal-proof-of-work-answer-from-a-miner
----

Anonymity

Broadcast -> Tor: https://en.wikipedia.org/wiki/Tor_(anonymity_network)
Explore: https://blockchain.info/tree/114688189
Zcoin: https://zcoin.io/wp-content/uploads/2016/11/zerocoinwhitepaper.pdf
(example graph isomophism)

Contracts

bitcoin: https://en.bitcoin.it/wiki/Contract
ethereum: https://ethereum.org/greeter