Bitcoin

David Malone
Hamilton Institute / Dept Maths&Stats
Maynooth University.

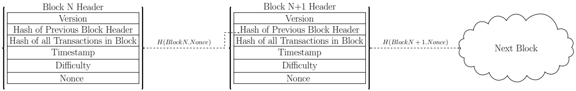
2018-01-25

Bitcoin Background

Bitcoin is a cryptocurrency that started around 2008–2009.

- Bitcoin provides a ledger of transactions.
- Each transaction has inputs and outputs[1].
- The value of inputs should be more than outputs.
- The transactions are gathered into blocks.
- The mining network competes to add blocks to the blockchain.
- Each block links to one immediately before it.

Originally got interested with Karl O'Dwyer as part of his work.



Block N Header

Version

Hash of Previous Block Header

Hash of all Transactions in Block

Timestamp

Difficulty

Nonce

$H(BlockN.Nonce)$

Block N+1 Header

Version

Hash of Previous Block Header

Hash of all Transactions in Block

Timestamp

Difficulty

Nonce

$H(BlockN+1.Nonce)$

Next Block

[1] In 0.00000001 BTC = 1 Satoshi.

Bitcoin Background

If you want to buy bitcoins, you need to get someone to make a transaction where you control the output.

If you want to sell bitcoins, you authorise a transaction from an output that you control.

Transactions have to be authorised, but you only want them to be authorised once. Without a central authority.

Transactions passed to peer-to-peer mining network for addition to blockchain.

Cryptographic Hash Functions

Bitcoin makes a lot of use of *hash functions*. Usually:

$$h : \{0,1\}^* \to \{0,1\}^N$$

So, it maps strings of bits[2] to a fixed length string.

- Collision resistant: hard to find x, x' with $h(x) = h(x')$.
- 2nd pre-image resistant: given x hard to find $x' \neq x$ with $h(x) = h(x')$.
- Pre-image resistant: given y hard to find x with $h(x) = y$.
- Basically, your best strategy should be brute-force guessing.

Bitcoin uses SHA256 as a hash function, usually applied twice. It also uses RIPEMD-160 in places.

[2] Sometimes bytes.

Public Key Signatures

- You want to be able to show approval.
- You generate a private key P and a public key p.
- Tell everyone the public key.
- *Signing*: To approve a message m calculate $\sigma = f(m, P)$.
- Tell everyone m and σ.
- *Verify:* Without knowing P, anyone can calculate $g(m, \sigma, p)$ to see if they match.

RSA and DSA are common signature schemes. They use one-way problems and often use hash functions too. Bitcoin uses EC-DSA.

Cryptography in Bitcoin

- Hashes used to identify things in Bitcoin.
- For example, bitcoin identities are hashes of public keys.
- Even transactions are identified by a hash of the transaction!

To output bitcoins to an identity, you actually say *to spend these bitcoins, the transaction must be signed and verify with a public key that hashes to this identity.*

So to spend Bitcoins, you need to know the private key corresponding to the outputs of a previous transaction, so you can generate the signature.

Coinbase

Where do the bitcoins come from in the first place?

- First transaction in each block is *coinbase*.
- It has no inputs.
- Input value is transaction fees plus block reward.
- Transaction fees are any spare from transaction in block.
- Block reward started at 50 BTC. Halves every 210,000 blocks.
- Currently 12.5 BTC, next halfing about June 2020[3].

The output of the coinbase is the reward for bitcoin mining. Aims to incentivise people to maintain blockchain.

[3] E.g. see `http://www.bitcoinblockhalf.com` for an estimate.

Hang on...

Why don't people generate blocks willy-nilly?

- When there are competing blocks, the longest chain wins.
- You want your blocks at the end.
- Make it computationally hard to chain blocks together.
- Prevents people whipping-up new version of history.

A block is a bit string, including hash of previous block, transactions and a unspecified value called a nonce.
Aim: Find a block x so that $h(x) < T$, for some target value T.

Mining

Mining bitcoin is the process of guessing an valid block x to solve $h(x) < T$. You pick a random nonce, permute transactions, ...

- You want your block to accepted into the chain.
- Other miners can easily check $h(x)$ and x.
- If block good, they are motivated to accept it (longer history).
- T is actually adapted over time.
- Recorded in block as difficulty $D = T_{\text{max}}/T$, where $T_{\text{max}} = (2^{16} - 1)2^{208}$.
- Aims to keep block discovery rate at 1 block / 10 min.
- As $h(x)$ looks random the average number of guesses $\approx D2^{32}$.

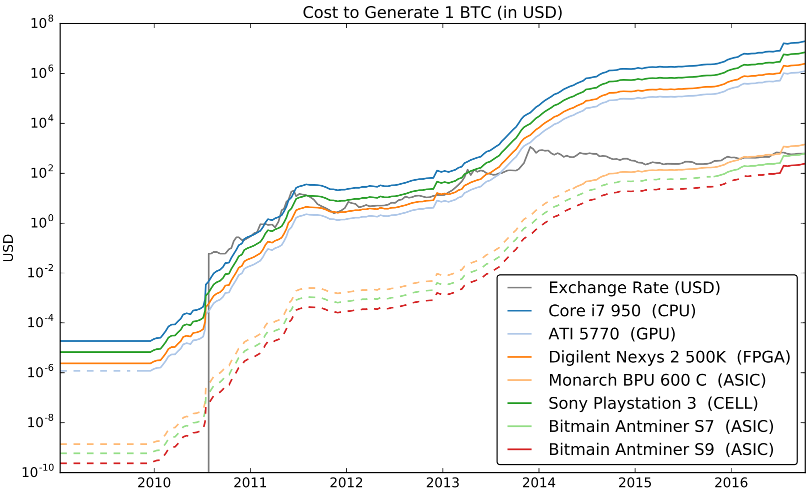
Mining arms race: CPUs, GPUs, FPGAs, ASICs.
Also, pools of miners.

Mining Hardware

Name	Type	Hash Rate R (Mhash/s)	Power Use P (W)	Energy Efficiency $\mathcal{E}$ (Mhash/J)	Cost ($)
Core i7 950	cpu	18.9	150	0.126	350
Atom N450	cpu	1.6	6.5	0.31	169
Sony Playstation 3	CELL	21.0	60	0.35	296
ATI 4850	gpu	101.0	110	0.918	45
ATI 5770	gpu	214.5	108	1.95	80
Digilent Nexys 2 500K	fpga	5.0	5	1	189
Monarch BPU 600 C	asic	600000.0	350	1714	2196
Antminer S9	asic	14000000.0	1400	10000	2400

Information available at sites like
`https://en.bitcoin.it/wiki/Mining_hardware_comparison`

Cost vs. Exchange Rate

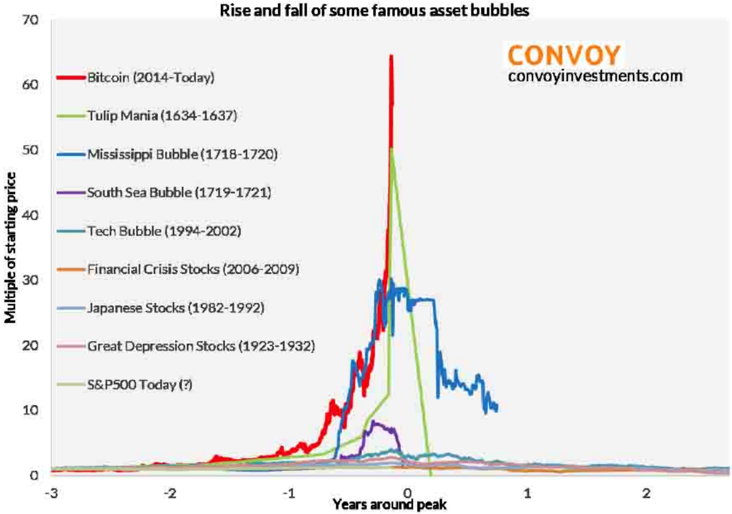


Global Consumption

- Realised we could also estimate global consumption.
- In 2014, was about 0.1–10GW in 2014.
- Ireland was using about 3-4GW at the time.
- Lots of interest in this estimate recently[4]
- Hash rate now about 20,000,000TH/s.
- 2GW with *best* hardware, no overheads.
- Number of transactions limited by max block size.

[4] `https://digiconomist.net`

Financial Side



Source: Elliot Wave International, Yale SOM, St. Louis FRED, GlobalFin, and Convoy analysis

Group DSA

Setup: Let G be a group, let $g \in G$ be an element of prime order q. Let $F : G \to \mathbb{Z}_q$ and pick a hash function h.

Keygen: Pick d and let $Q = g^d$. Q is the public key.

Sign: Let $z = h(m)$ and choose non-zero $k \in \mathbb{Z}_q$ randomly. Let $r = F(g^k) \mod q$ and $s = k^{-1}(z + rd) \mod q$. If r or s are zero, try again. $\sigma = (r, s)$.

Verify: To verify, check r, s non-zero. Set $z = h(m)$. Find $w = s^{-1} \mod q$. Let $u_1 = zw \mod q$ and $u_2 = rw \mod q$. Check if $F(g^{u_1} Q^{u_2}) = r$.

For G an eliptic curve group and $F(x, y) = x$ you get ECDSA.
For $G = \mathbb{Z}_p$ and $F(g) = g \mod q$ you get DSA.