Does Bitcoin Use As Much Energy As Ireland?

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

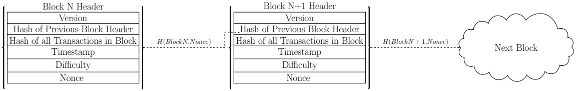
2019-11-11

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

Block N+1 Header
Version
Hash of Previous Block Header
Hash of all Transactions in Block
Timestamp
Difficulty
Nonce

[1] In 0.00000001 BTC = 1 Satoshi.

And? So What?

- We already have ledgers!
- They already have rules!
- *They are maintained by trustworthy people.*

Bitcoin: maintain a ledger with an untrusted group.
How do you decide which ledger is the real one?

What could go wrong?

It's just a list of transactions.

1. Unauthorised transaction?
2. Add/delete authorised transaction?

Second is called *double spending*.

Rules:

1. Transactions should be signed.
2. Presented with two versions of history, choose the longest valid one.

Bitcoin Operation

Transactions passed to peer-to-peer “mining” network for addition to blockchain. Everyone can check they are signed.

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

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

Longer histories are better, so better make it hard to create long blockchains.

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 s from m and P.
- Tell everyone m and s.
- *Verify:* Without knowing P, anyone can check s matches m using p.

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

Cryptographic Hash Functions

Functions:

$$f(x) = 2x + 4.$$

Can solve $f(x) = 8$ easily.

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

- They take in arbitrary data, give fixed length output.
- Hard to forge.
- Usually h is chosen to behave like a random function.
- You can depend on output looking uniformly random.
- Best strategy to solve $h(x) = y$ for x is guess.

Designed so usual tricks don't work.

Hash Functions 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 normal inputs.
- Input: 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 May 2020[2].

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

[2] 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 chunk of data, 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: Proof-of-Work

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).
- How much work to find a solution?

As hashes look random, this looks like tossing a very biased coin. Calculating average number of hashes before success is easy.

Difficulty

Bitcoin wants to keep this problem hard, but not too hard.

- T is actually adapted over time.
- Aims to keep block discovery rate at 1 block / 10 min.
- Adjusts T every 2016 blocks (roughly 2 weeks).
- Recorded in block: $D = T_{\text{max}}/T$ called *difficulty*[3].
- You might expect miners to respond to difficulty.

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

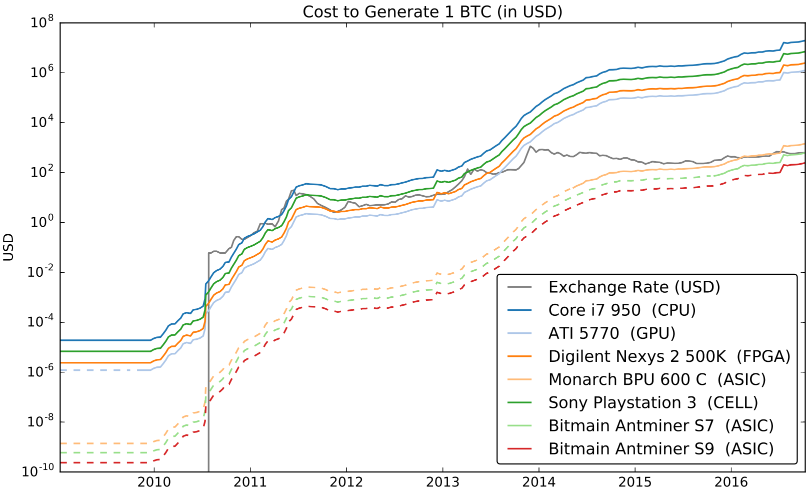
[3] Where $T_{\text{max}} = (2^{16} - 1)2^{208}$

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

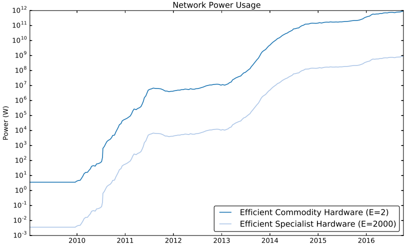
Information available at sites like
`https://en.bitcoin.it/wiki/Mining_hardware_comparison`

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 *electricity* at the time.
- Lots of interest in this estimate recently[4].
- Hash rate[5] now about 91,000,000TH/s.
- ≈9GW with *best* hardware, no overheads.

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

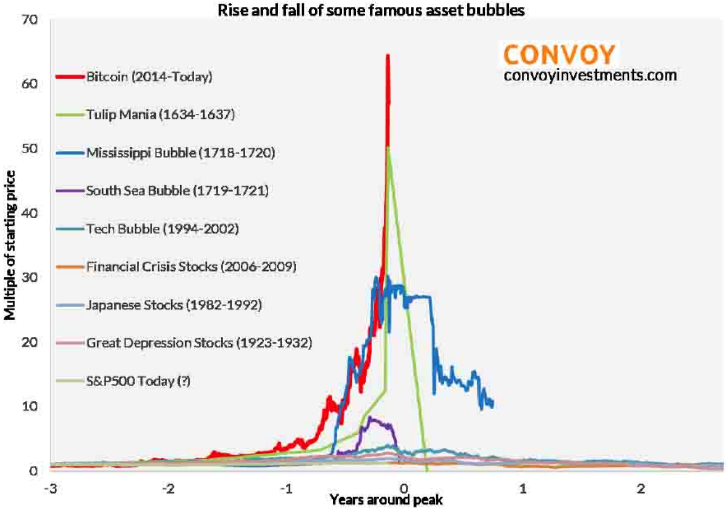
[5] `https://blockchain.info/charts/hash-rate`

Financial Side

- Don't take financial advice from me.
- Did some economics in TY in secondary school.
- Peaked at almost \$20,000 in December 2017[6].
- Dipped to almost \$3,000, now about levelled out about \$8,000–9,000.
- Volatile.
- Many copy coins.
- Some with interesting features.

[6] https://blockchain.info/charts/market-price

Financial Side



Rise and fall of some famous asset bubbles

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

Conclusion

- Dead clever way of keeping a ledger.
- Uses a lot of electricity.
- Haven't talked about Proof-of-Stake.
- Haven't talked about deanonymisation.
- Haven't talked about security analysis.
- Haven't talked about block size related problems.