# *Bitcoin and its Energy Usage*

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

2023-06-16


nu te huur

# *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. (Why?)
- Each block has a summary of one immediately before it.

Changing history is really difficult!

$$\leftarrow \boxed{\text{Block 98}} \leftarrow \boxed{\text{Block 99}} \leftarrow \boxed{\text{Block 100}} \leftarrow \boxed{\text{Block 101}}.$$

[1] In 0.00000001 BTC = 1 Satoshi.

# *Coinbase*

Where do the bitcoins come from in the first place?

- First transaction in each block is *coinbase*.
- Input value is transaction fees plus block reward.
- Transaction fees are any spare from transaction in block.
- Block reward started at 50 BTC. Halves roughly every 4 years.
- Currently 6.25 BTC, next halfing late April 2024[2].

The output of the coinbase is the reward for bitcoin *mining*.
People building the blockchain get free bitcoins!

[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 hard to chain blocks together.
- Prevents people giving themselves lots of bitcoins . . .
- . . . or changing history.

Bitcoin sets puzzles to decide.

# *Mathematical Functions*

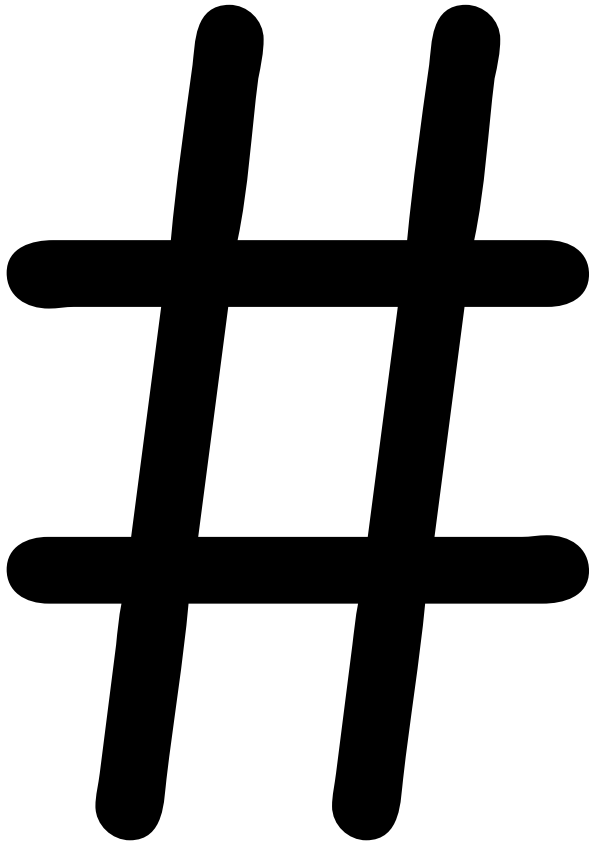
- Functions are rules, input $\rightarrow$ consistent output.
- We tell you about functions like $f(x) = x^2 - 5x + 6$.
- You can do things like solve $f(x) = 0$.

$$f(x) = 0 \Leftrightarrow x^2 - 5x + 6 = (x - 2)(x - 3) = 0$$

So $x = 2$ or $x = 3$.

- These are the nice functions.

With a bit of work, you could probably find an $x$ value so that $f(x) < 0.1$. This is the type of puzzle Bitcoin uses!



# *Cryptographic Hash Functions*

A hash function $h(x)$ takes in any binary data $x$ and gives you a list of 0s and 1s as output.

Bitcoin uses SHA256 as a hash function, usually applied twice.[3]

Designed to be horrible! Looks random!

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

[3] There's a YouTube video where someone does it by hand `https://www.youtube.com/watch?v=y3dqhixzGVo`.

# *Mining*

Mining bitcoin is the process of guessing an valid block $x$ find $h(x)$ so it starts with a lot of zeros (target).

- You want your block to accepted into the chain.
- If you tell them $x$ miners can easily check $h(x)$.
- If block good, they are motivated to accept it (longer history).
- Target changed to keep block rate at 1 block / 10 min.
- How many guesses needed?

Use probability and target from blocks to figure it out!

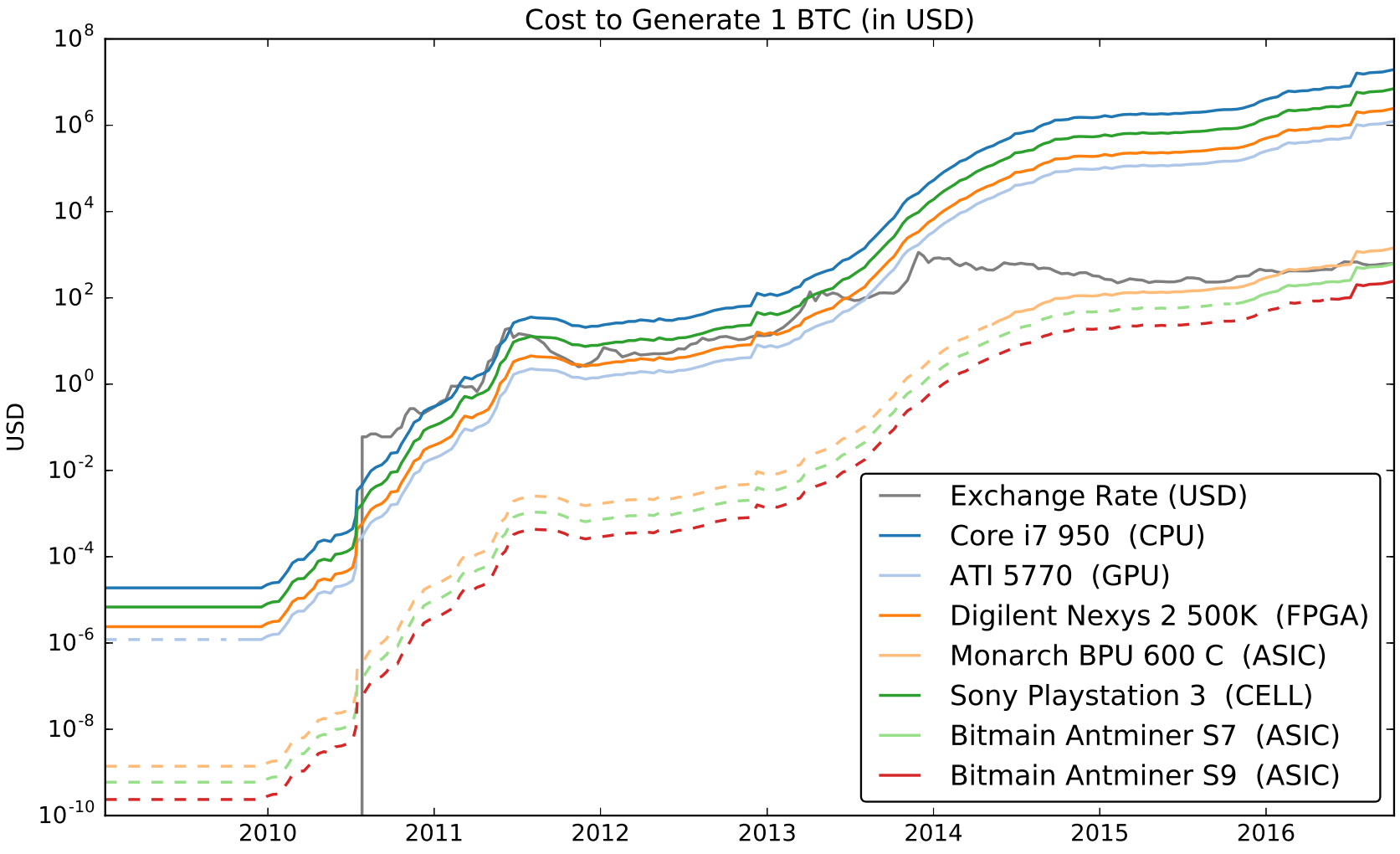
# *How Much Power?*

| 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*

- In 2014, was about 0.1–10GW in 2014.
- Ireland was using about 3–4GW the time.
- Lots of interest in this estimate recently[4]
- Hash rate now about 394,000,000TH/s[5].
- 35GW with *best* hardware, no overheads.

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

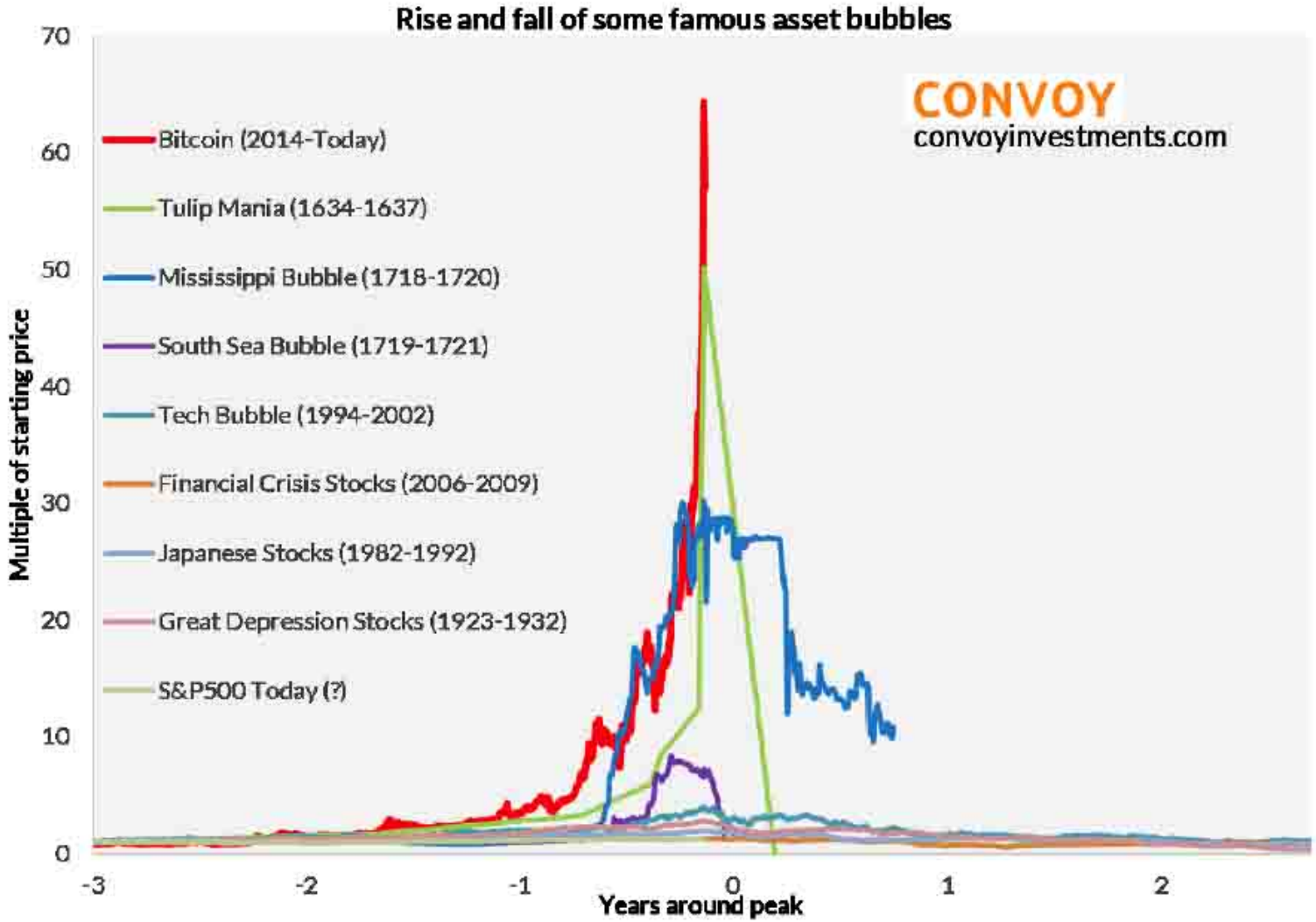
[5] `https://www.blockchain.com/explorer/charts/hash-rate`

# *Conclusion*

- Clever way of keeping a ledger using cryptography.
- Keeps track of imaginary money.
- Uses a lot of electricity[6].
- Some other cryptocurrencies are trying to fix this.

[6] Original paper at
https://mural.maynoothuniversity.ie/6009/1/DM-Bitcoin.pdf

# *Why is it Valuable?*




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