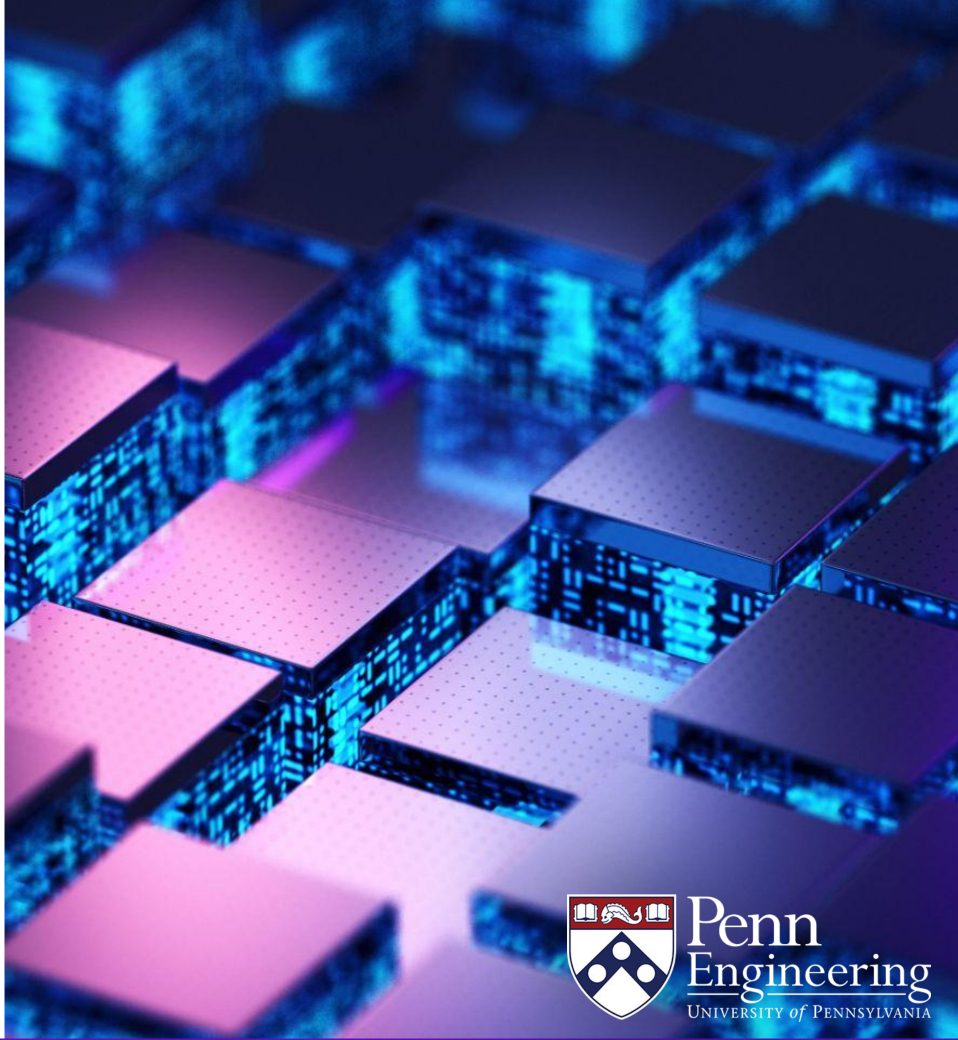
EAS 5830: BLOCKCHAINS

The Bitcoin Mining Economy

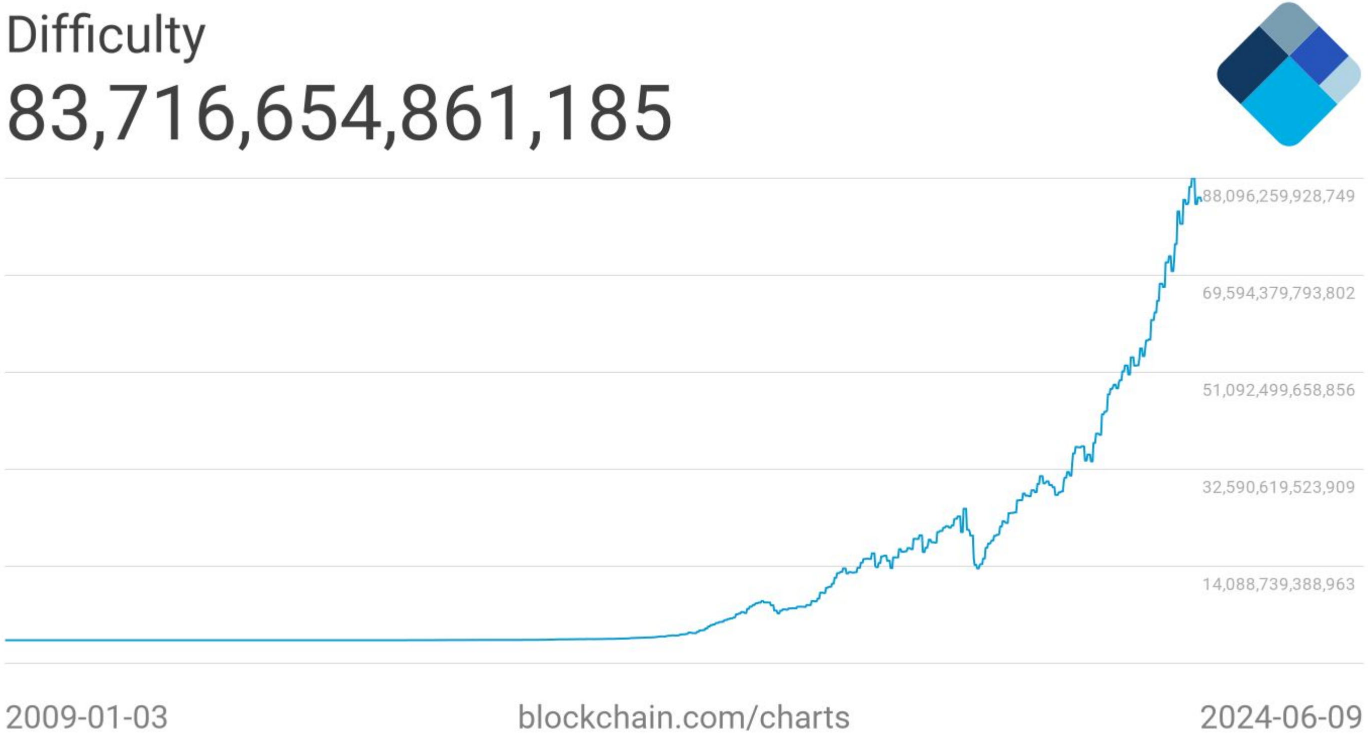
Professor Brett Hemenway Falk



Penn Engineering
UNIVERSITY of PENNSYLVANIA

Difficulty

- A bitcoin block is only “valid” if its hash is less than a “target” value
- All miners are doing this simultaneously and independently by hashing candidate blocks
- Initial target: `0x00000000ffff0000000000000000000000000000000000000000000000000000`
  - On average about 2^{32} ~ 4 billion trials
- Difficulty defined to be: initial target / current target
- Current difficulty has increased to about 83.0T



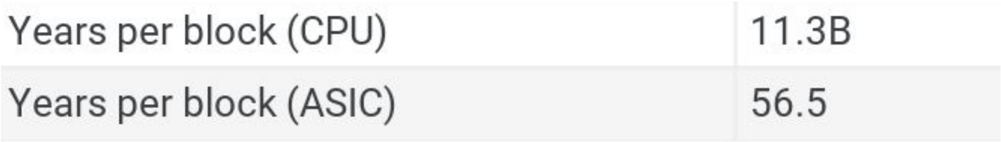
Difficulty

83,716,654,861,185

blockchain.com/charts

Difficulty

- Current difficulty ~ 83.0T
  - (Current Difficulty)·(Base Difficulty) ~ 356.5*10^21 hashes on average before finding a solution
- A good CPU can do ~ 1M hashes / second
- ASICs can do ~ 200 T hashes / second



Years per block (CPU)	11.3B
Years per block (ASIC)	56.5

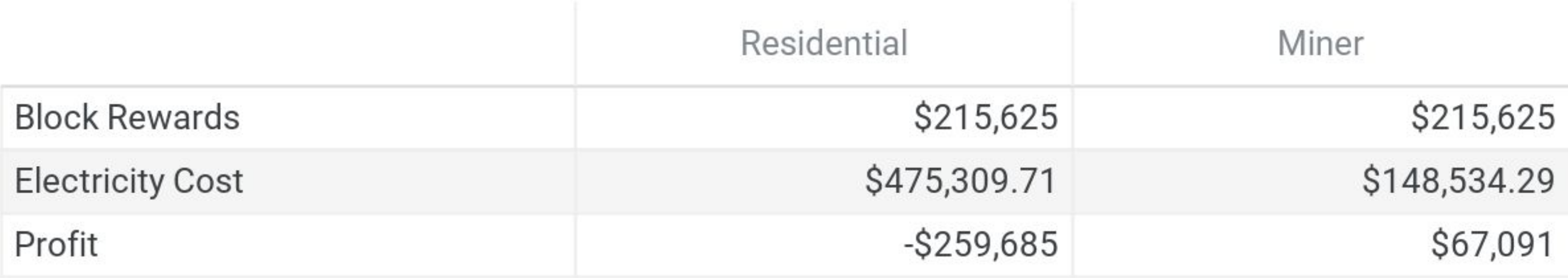
ANTMINER
Reset
Fault
Normal

Why mine?

- When you mine a block you collect:
  - Block rewards
    - Block rewards halve every 210,000 blocks (approximately every 4 years)
      - Block rewards were initial 50 BTC / block
      - 50 → 25 → 12.5 → 6.25 → 3.125
  - Transaction fees

Basic economics

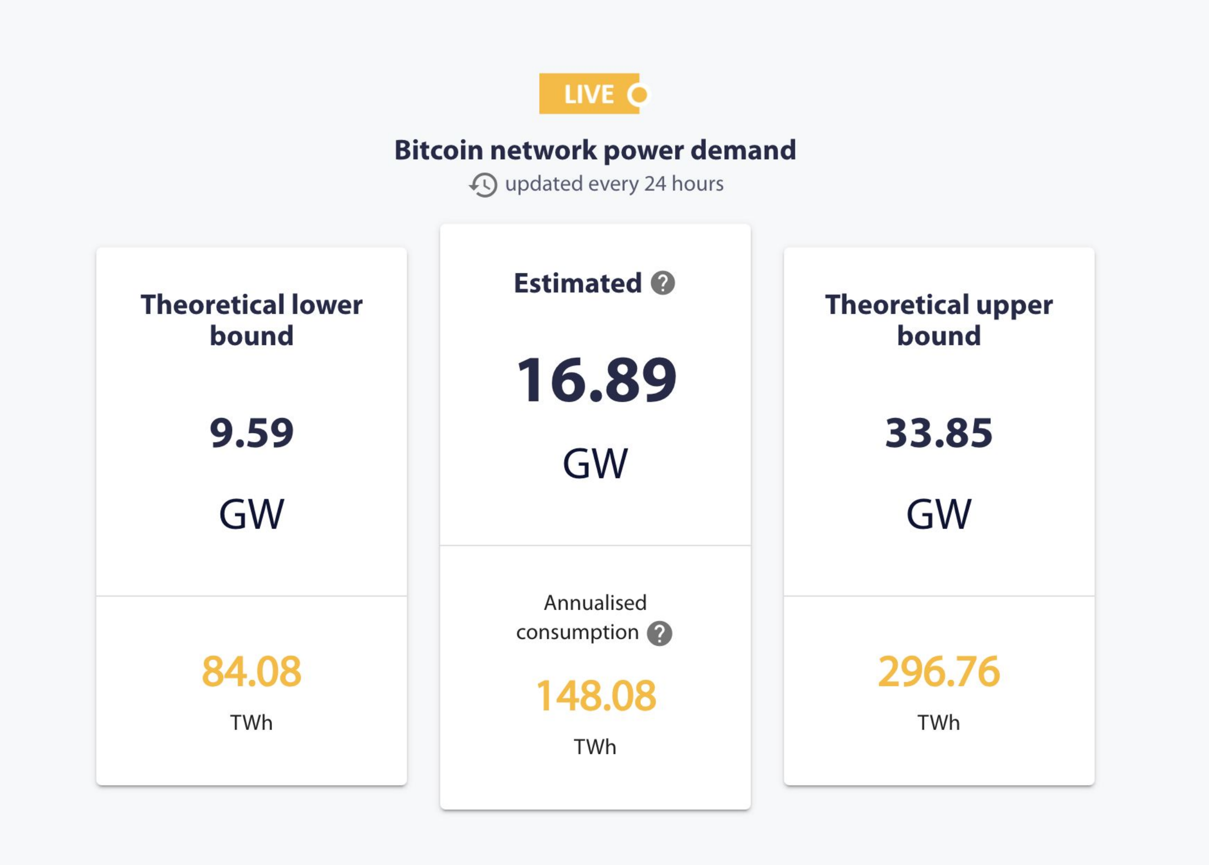
- Best ASIC miners run at ~30 J / TH
- 356.5*10^21 Hashes required to find a block
- (Expected number terahashes)·(Joules / TH) = 10.7T Joules / Block
    - (1 kWH = 3.6M J)
- Average residential energy cost is $0.16 / kWH
- Average Bitcoin miner pays about .05 kWH for electricity
- Current Bitcoin block rewards are 3.125 BTC



	Residential	Miner
Block Rewards	$215,625	$215,625
Electricity Cost	$475,309.71	$148,534.29
Profit	-$259,685	$67,091

Energy usage

- Bitcoin network computes (on average) 356.5*10^21 hashes every ten minutes
- Best ASIC miners run at ~ 30J / TH
- ~ 18GW (if all mining was done with best ASICs)
    - Recall 1 watt = 1 joule per second



LIVE

Bitcoin network power demand

updated every 24 hours

Theoretical lower bound	Estimated	Theoretical upper bound
9.59 GW	16.89 GW	33.85 GW
	Annualised consumption	
84.08 TWh	148.08 TWh	296.76 TWh

Comparisons

- Bitcoin uses approximately as much energy as Poland (170 TWH)
- Netflix required .451 TWH in 2019
  - Maybe up to 94 TWH?
- Facebook 15 TWH
- Training GPT-4 might have required 7.2 GWH
- By 2027 AI might consume 134 TWH

Why not change?

- Economics
  - Miners have invested billions of dollars in mining hardware, they don’t want that investment to be wasted
- Stability
  - It’s hard to get people to upgrade to new versions
  - The anti-upgrade mentality is necessary to keep supply from increasing
- Anonymity
  - It’s easier to mine anonymously
    - Staking requires buying stake
    - Mining can be done by anyone who can get electricity

Variability of rewards

- Expected rewards
  - (Probability of mining a block) · (Rewards for mining a block)
  - Probability is very low
  - Rewards are very high
- This means the *variance* in rewards is very high
  - If you get value v with probability p, and 0 otherwise
    - Expectation is $v \cdot p$
    - Variance is $v^2 \cdot p \cdot (1-p)$
- **Decreasing v and increasing p keeps expectation the same, but decreases variance**

Mining pools

- Miners pool together and share rewards
- Same expected revenue
- Lower variance

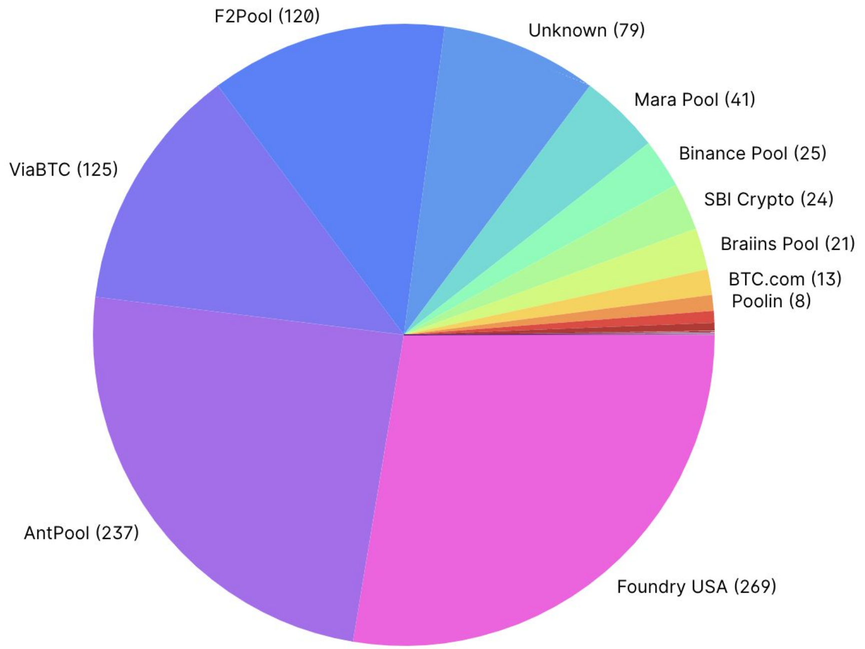
Operating mining pools

- Pool operator sends a block template to miners
- Miners iterate over nonces
  - Bitcoin only accepts with block with ~78 leading zeros
  - Mining pool accepts “partial” solutions with ~32 leading zeros
- When a pool finds a block rewards are split between all pool members
  - Each member receives rewards proportional to number of partial solutions they have submitted

Attacks on mining pools

- Mine on different pools – submit “partial” proofs to two pools
  - **Fix**: Has a unique block template, only accept partial proofs with correct template
- Withhold winning block – if a pool member finds a valid block, send it directly to the blockchain, don’t send it to the pool
  - **Fix**: Pool template includes coinbase payment to pool, not to member
  - **Problem**: Miner has to trust pool (but pool does **not** have to trust miner)

Mining Pools



Centralization

- If pool operator chooses transactions, then small number of operators can censor Bitcoin transactions
- If individual pool members choose transactions, pool cannot easily censor transactions
- Bitcoin Explained has a good description of Stratum V2