CBS COPENHAGEN BUSINESS SCHOOL
HANDELSHØJSKOLEN

Elective Course on Mastering Blockchain: Foundations to Consensus, session-07

Bitcoin Mining Fundamentals and Proof-of-work

Raghava Mukkamala

Associate Professor & Director, Centre for Business Data Analytics
Copenhagen Business School, Denmark
Email: rrm.digi@cbs.dk, Centre: https://cbsbda.github.io/

Course Coordinator at SRMIST:

Prof. K. Shantha Kumari

Associate Professor
Data Science and Business Systems Department,
SRM Institute of Science and Technology, India
Shanthak@srmist.edu.in

EQUIS ACCREDITED AACSB ACCREDITED ASSOCIATION AMBA ACCREDITED CEMS PIM

Outline

- Bitcoin Mining Basics
- Bitcoin Mining Hardware
- Mining Pools

Bitcoin Mining Basics

Image by mohamed_hassan from Pixabay

Slides based on Bitcoin and Cryptocurrency Technologies: http://bitcoinbook.cs.princeton.edu/

CBS

How is decentralized consensus achieved?

- Bitcoin's decentralized consensus emerges from the interplay of four processes that occur independently on nodes across the network
    - Independent verification of each transaction, by every full node, based on a comprehensive list of criteria
    - Independent aggregation of those transactions into new blocks by mining nodes, coupled with demonstrated computation through a Proof-of-Work algorithm
    - Independent verification of new blocks and assembly into a chain by nodes
    - Independent selection, by every node, of the chain with the most cumulative computation (longest chain) demonstrated through Proof-of-Work

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.". p.217

Recap: How Transactions are created

- A locking script is a spending condition placed on an output
- Locking script is called a scriptPubKey, as it contains a public key
- An unlocking script is a script that “solves,” or satisfies, the conditions placed on output by a locking script.
- it is called scriptSig, as it contained a digital signature.

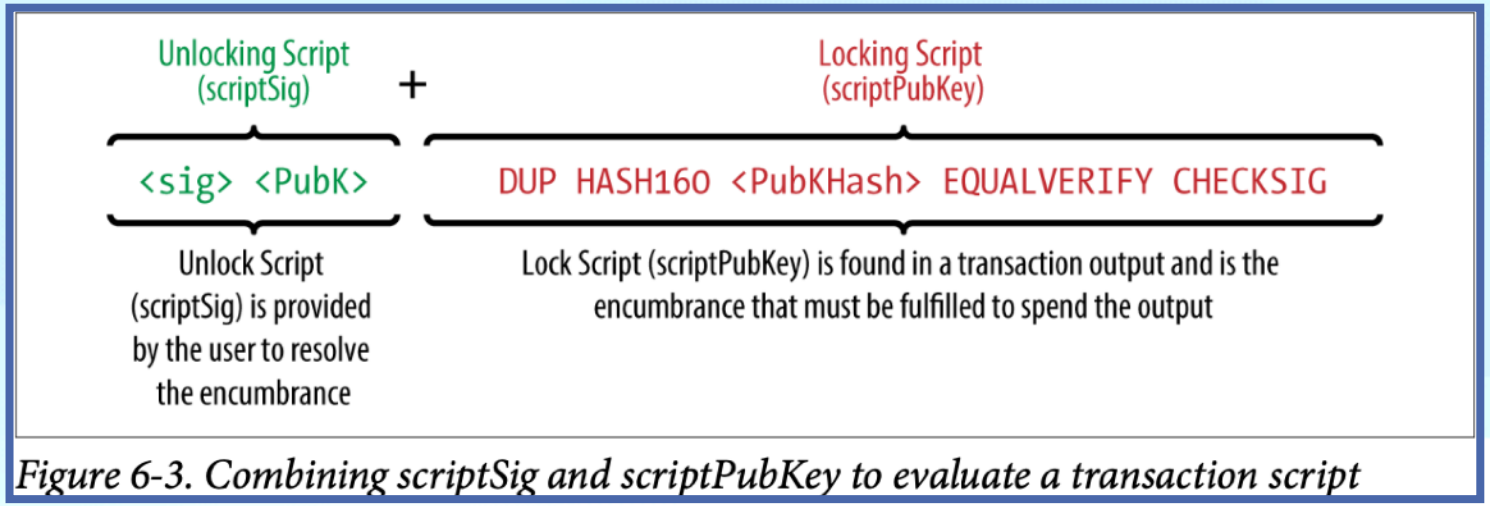


Figure 6-3. Combining scriptSig and scriptPubKey to evaluate a transaction script

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.”. p.217

Independent Verification of Transactions

- If you are spending coins, wallet software creates transactions by unlocking scripts
- Transactions is sent to the neighboring nodes in the network to propagate across the entire network.
- Every node verifies every transaction against a long checklist of criteria:

- The transaction's syntax and data structure must be correct.
- Neither lists of inputs or outputs are empty.
- The transaction size in bytes is less than `MAX_BLOCK_SIZE`.
- Each output value, as well as the total, must be within the allowed range of values (less than 21m coins, more than the *dust* threshold).
- None of the inputs have hash=0, N=–1 (coinbase transactions should not be relayed).
- `nLocktime` is equal to `INT_MAX`, or `nLocktime` and `nSequence` values are satisfied according to `MedianTimePast`.
- The transaction size in bytes is greater than or equal to 100.
- The number of signature operations (SIGOPS) contained in the transaction is less than the signature operation limit.

- The unlocking script (`scriptSig`) can only push numbers on the stack, and the locking script (`scriptPubkey`) must match `isStandard` forms (this rejects "non-standard" transactions).
- A matching transaction in the pool, or in a block in the main branch, must exist.
- For each input, if the referenced output exists in any other transaction in the pool, the transaction must be rejected.
- For each input, look in the main branch and the transaction pool to find the referenced output transaction. If the output transaction is missing for any input, this will be an orphan transaction. Add to the orphan transactions pool, if a matching transaction is not already in the pool.
- For each input, if the referenced output transaction is a coinbase output, it must have at least `COINBASE_MATURITY` (100) confirmations.
- For each input, the referenced output must exist and cannot already be spent.
- Using the referenced output transactions to get input values, check that each input value, as well as the sum, are in the allowed range of values (less than 21m coins, more than 0).
- Reject if the sum of input values is less than sum of output values.
- Reject if transaction fee would be too low (`minRelayTxFee`) to get into an empty block.
- The unlocking scripts for each input must validate against the corresponding output locking scripts.

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.". p.217

Aggregating Transactions into Blocks

- After validating transactions, a bitcoin node will add them to the memory pool, or transaction pool, where transactions wait until they can be included (mined) into a block.
- Nodes collect, validate, and relay new transactions. However, nodes will then aggregate these transactions into a candidate block to create a new block by solving the hash puzzle.
- If a new block arrives, nodes end the competition of making a new block and restart their computation for a new one by assigning the newly listed block as the previous one.
- This process is reset in every 10 mins as a new block is generated approximately every 10 mins.

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.". p.217

Mining Bitcoins in 6 easy steps

1. Join the network, listen for transactions
    a. Validate all proposed transactions
2. Listen for new blocks, maintain block chain
    a. When a new block is proposed, validate it
3. Assemble a new valid block
4. Find the nonce to make your block valid
5. Hope everybody accepts your new block
6. Profit!

Useful to Bitcoin network

The Coinbase Transaction

Table 10-1. The structure of a "normal" transaction input

Size	Field	Description
32 bytes	Transaction Hash	Pointer to the transaction containing the UTXO to be spent
4 bytes	Output Index	The index number of the UTXO to be spent, first one is 0
1–9 bytes (VarInt)	Unlocking-Script Size	Unlocking-Script length in bytes, to follow
Variable	Unlocking-Script	A script that fulfills the conditions of the UTXO locking script
4 bytes	Sequence Number	Currently disabled Tx-replacement feature, set to 0xFFFFFFFF

Table 10-2. The structure of a coinbase transaction input

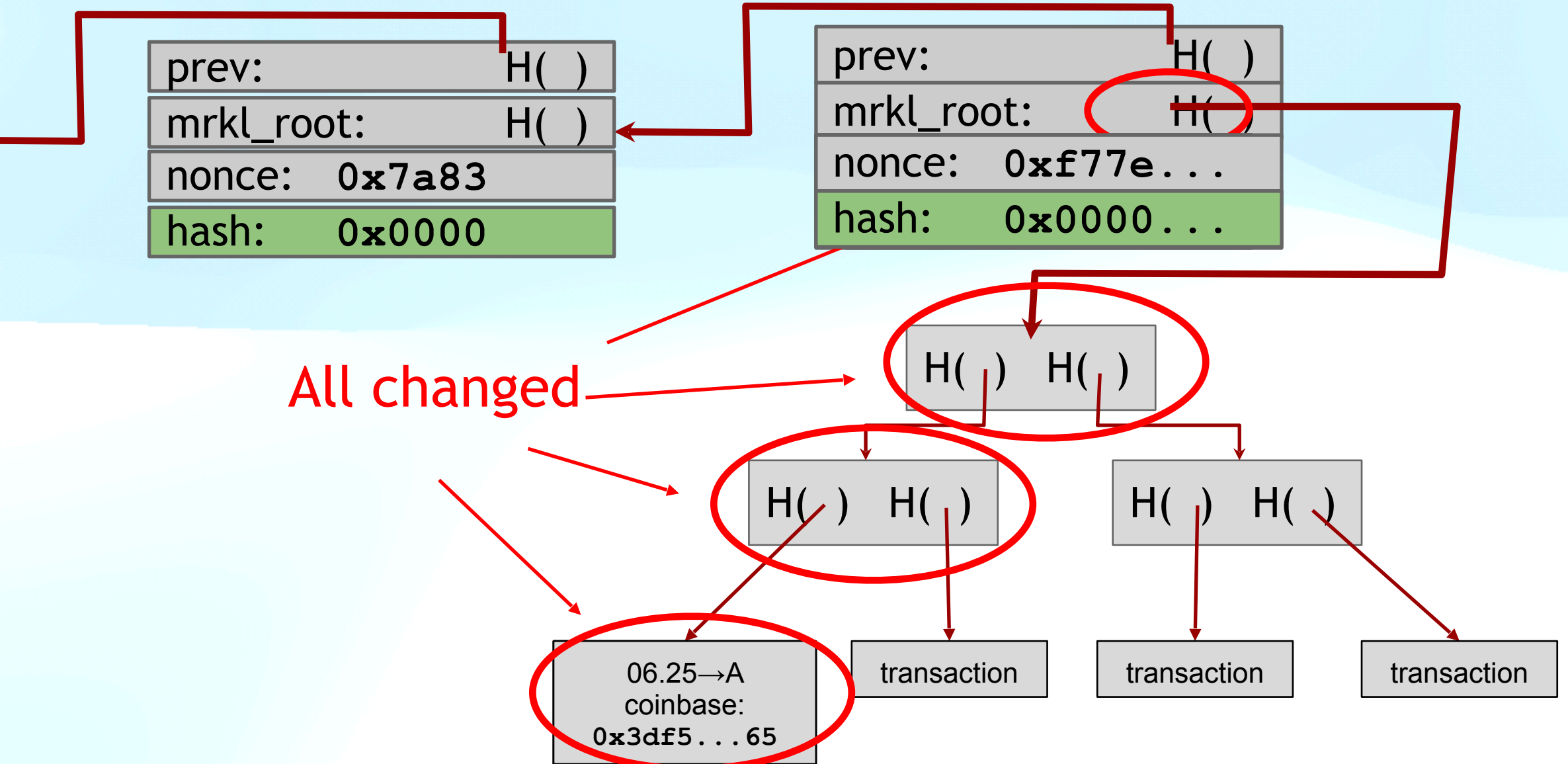
Size	Field	Description
32 bytes	Transaction Hash	All bits are zero: Not a transaction hash reference
4 bytes	Output Index	All bits are ones: 0xFFFFFFFF
1–9 bytes (VarInt)	Coinbase Data Size	Length of the coinbase data, from 2 to 100 bytes
Variable	Coinbase Data	Arbitrary data used for extra nonce and mining tags. In v2 blocks; must begin with block height
4 bytes	Sequence Number	Set to 0xFFFFFFFF

https://www.blockchain.com/explorer/blocks/btc/779184

https://blockchain.info/rawblock/00000000000000000001608696a871062ecc9264d9f96dd31fb993234b1043f

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.". p.217

Finding a valid block



Target Representation

In Example 10-3, we saw that the block contains the target, in a notation called "target bits" or just "bits," which in block 277,316 has the value of `0x1903a30c`. This notation expresses the Proof-of-Work target as a coefficient/exponent format, with the first two hexadecimal digits for the exponent and the next six hex digits as the coefficient. In this block, therefore, the exponent is `0x19` and the coefficient is `0x03a30c`.

The formula to calculate the difficulty target from this representation is:

```
target = coefficient * 2^(8 * (exponent - 3))
```

Using that formula, and the difficulty bits value 0x1903a30c, we get:

```
target = 0x03a30c * 2^(0x08 * (0x19 - 0x03))^

=> target = 0x03a30c * 2^(0x08 * 0x16)^

=> target = 0x03a30c * 2^0xB0^
```

which in decimal is:

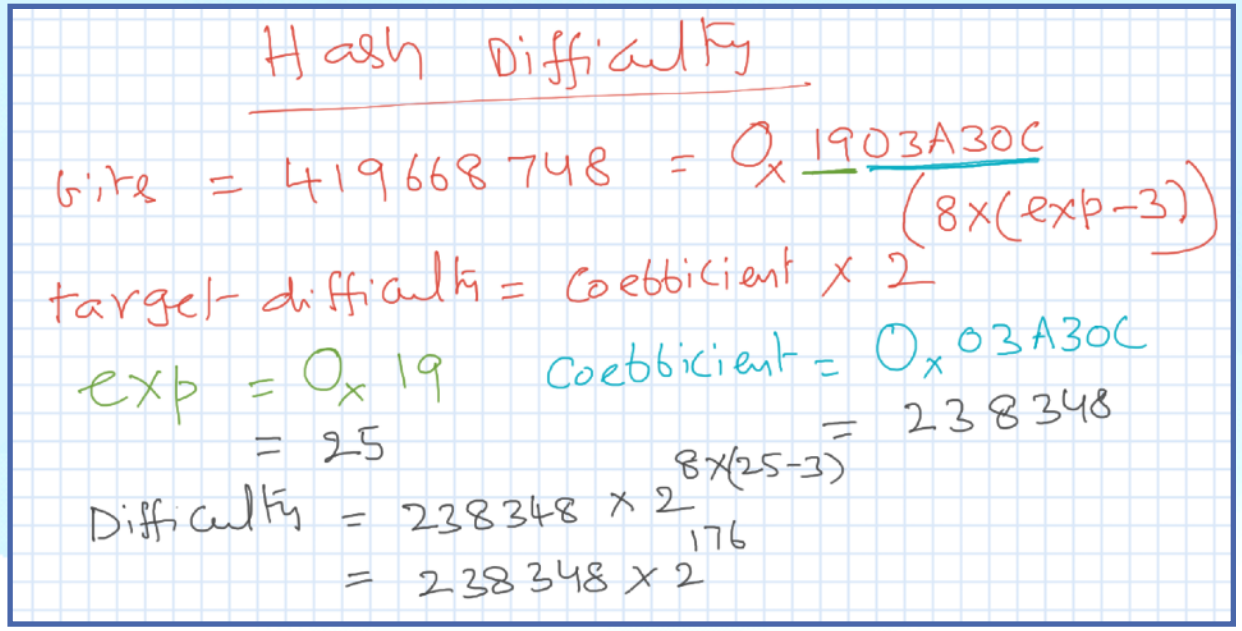
```
=> target = 238,348 * 2^176^

=> target =
22,829,202,948,393,929,850,749,706,076,701,368,331,072,452,018,388,575,715,328
```

switching back to hexadecimal:

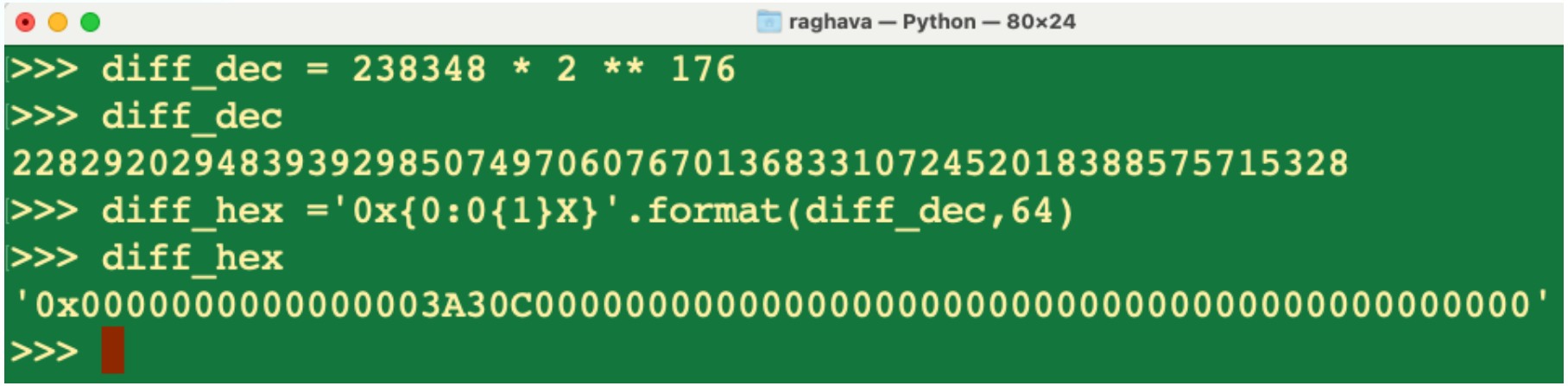
```
=> target = 0x0000000000000003A30C0000000000000000000000000000000000000000000
```


Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.". p.235

Hash Difficulty for Block 277316



https://www.blockchain.com/explorer/blocks/btc/277316



https://blockchain.info/rawblock/000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4

Hash Difficulty for Block 277316

raghava — Python — 80×24

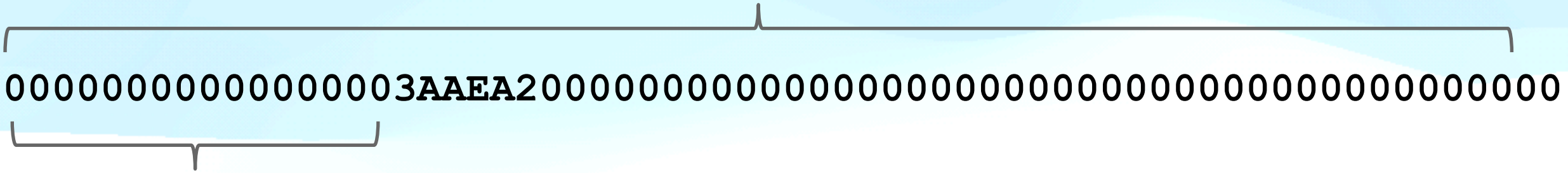
```
>>> block_hash_277316_hex = '0x00000000000000001b6b9a13b095e96db41c4a928b97ef2d94
4a9b31b2cc7bdc4'
>>> block_hash_277316_hex
'0x00000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4'
>>> block_hash_277316_dec = int(block_hash_277316_hex, base=16)
>>> block_hash_277316_dec
107575085536129821207562387057422357917467417853866692929 96
>>> diff_dec
22829202948393929850749706076701368331072452018388575715328
>>> diff_dec > block_hash_277316_dec
True
>>> print(diff_dec - block_hash_277316_dec)
120716943947809477299934673709591325393257102330019064223 32
>>>
```

https://www.blockchain.com/explorer/blocks/btc/277316

Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.". p.235

Mining difficulty “target” (2014-08-07)

256 bit hash output

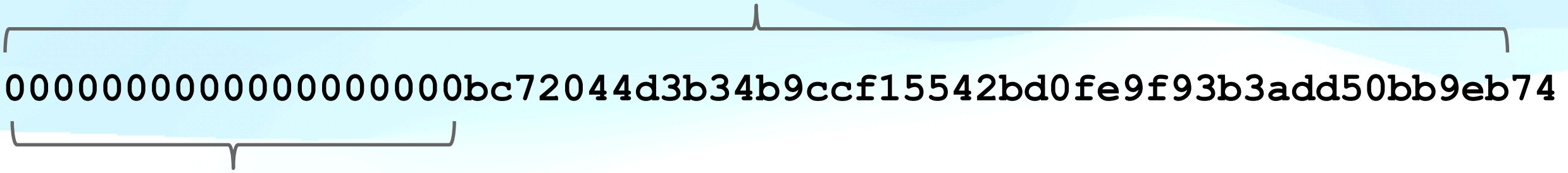


$$\text{difficulty} = 2^{66.2}$$

$$= 84,758,978,290,086,040,000$$

Mining difficulty “target” (2023-03-03)

256 bit hash output

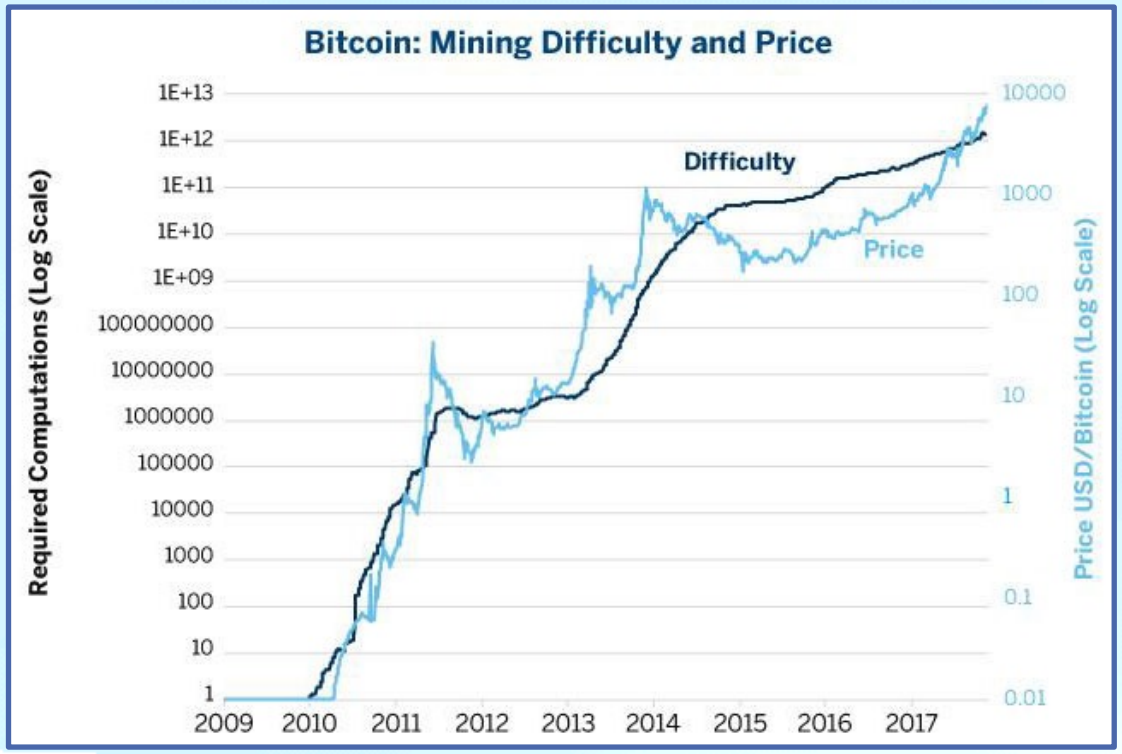


78+ bits of leading zeroes required

Current difficulty = $2^{78.2}$

= 12,759,819,404,408 84,758,978,290,086,040,000

=1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976 (as of now)



2. Mining Difficulty (Hash Difficulty)

The **mining difficulty** refers to how hard it is to find the correct hash for a new block in the Bitcoin network.

- **Target Hash**: The Bitcoin protocol sets a target hash that miners need to hit or go below to successfully mine a new block. The goal for miners is to find a nonce (random number) that, when combined with the transaction data and hashed, results in a value lower than the current target.

1. Hash Rate

The **hash rate** refers to the computational power used by miners to process transactions and secure the Bitcoin network. It measures how many hash calculations a miner (or group of miners) can perform per second while trying to solve the cryptographic puzzle required to add a new block to the blockchain.

https://data.bitcoinity.org/bitcoin/hashrate/6m?c=m&g=15&t=a

https://en.bitcoinwiki.org/wiki/Difficulty_in_Mining

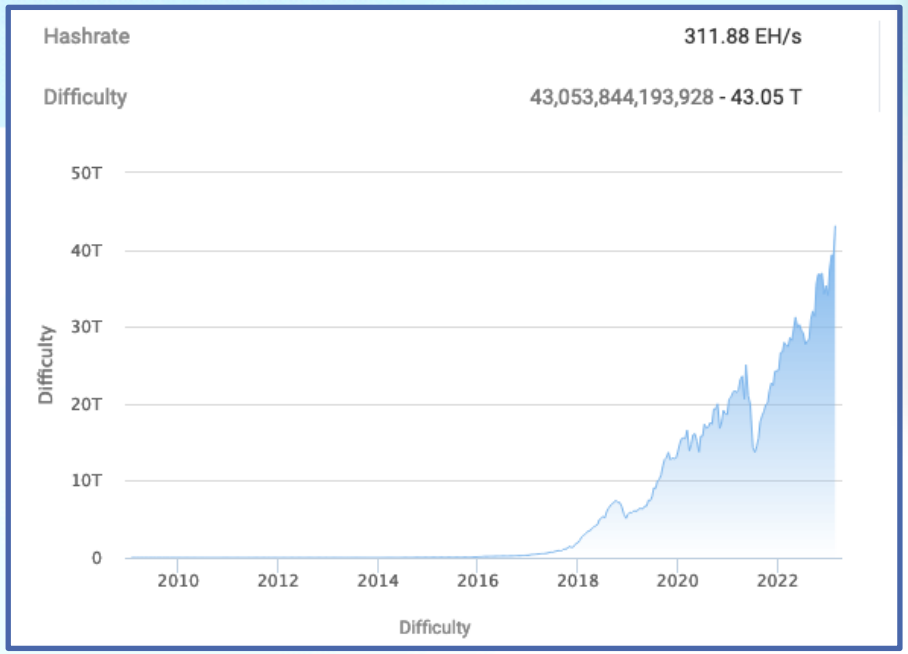
Hash rate is a unit measured in hashes per second or [h/s] and here are some usual denominations used to refer it.

Hash rate denominations

- 1 kH/s is 1,000 (one thousand) hashes per second
- 1 MH/s is 1,000,000 (one million) hashes per second.
- 1 GH/s is 1,000,000,000 (one billion) hashes per second.
- 1 TH/s is 1,000,000,000,000 (one trillion) hashes per second.
- 1 PH/s is 1,000,000,000,000,000 (one quadrillion) hashes per second.
- 1 EH/s is 1,000,000,000,000,000,000 (one quintillion) hashes per second.

Hash rate, miner's reward, and difficulty are interdependent on each other in various ways. Whenever Bitcoin network's difficulty goes up more hash rate is required to mine/find the blocks and as result miners earn the block reward of 12.5 BTC plus the transaction fees.

Interestingly, the Bitcoin network's difficulty goes up because of more miners joining the network and thus the hash power needs to be increased (i.e. more computational guesses needs to be made per second to find the solution).



What is the current hash rate and hash difficulty for Bitcoin?

Searched 6 sites

As of early September 2024, the **Bitcoin network hash rate** is around **642-653 exahashes per second (EH/s)**, reflecting the combined computational power of miners securing the network. This is down from a peak of **879 EH/s** reached in July 2024. The hash rate fluctuates as miners join or leave the network, depending on factors like profitability and hardware efficiency.

Meanwhile, the **mining difficulty** is currently around **89.5 trillion (T)**. Difficulty adjusts approximately every two weeks to ensure that new blocks are added to the blockchain every 10 minutes on average. The next difficulty adjustment is expected to increase slightly by about 2.65%, continuing the trend of rising difficulty due to the growing hash rate(CoinWarz, CoinWarz, Crypto Trust, Hashrate Index).

These two metrics are crucial because they ensure Bitcoin's security and stability. A higher hash rate increases the network's security, while difficulty ensures blocks are mined at a consistent pace, regardless of how much computational power is being used.

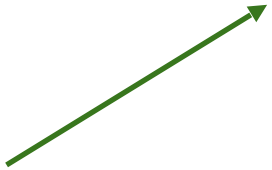
https://www.quora.com/What-is-the-difference-between-hash-rate-and-difficulty-in-cryptocurrency-mining

https://en.bitcoinwiki.org/wiki/Difficulty_in_Mining

Setting the mining difficulty

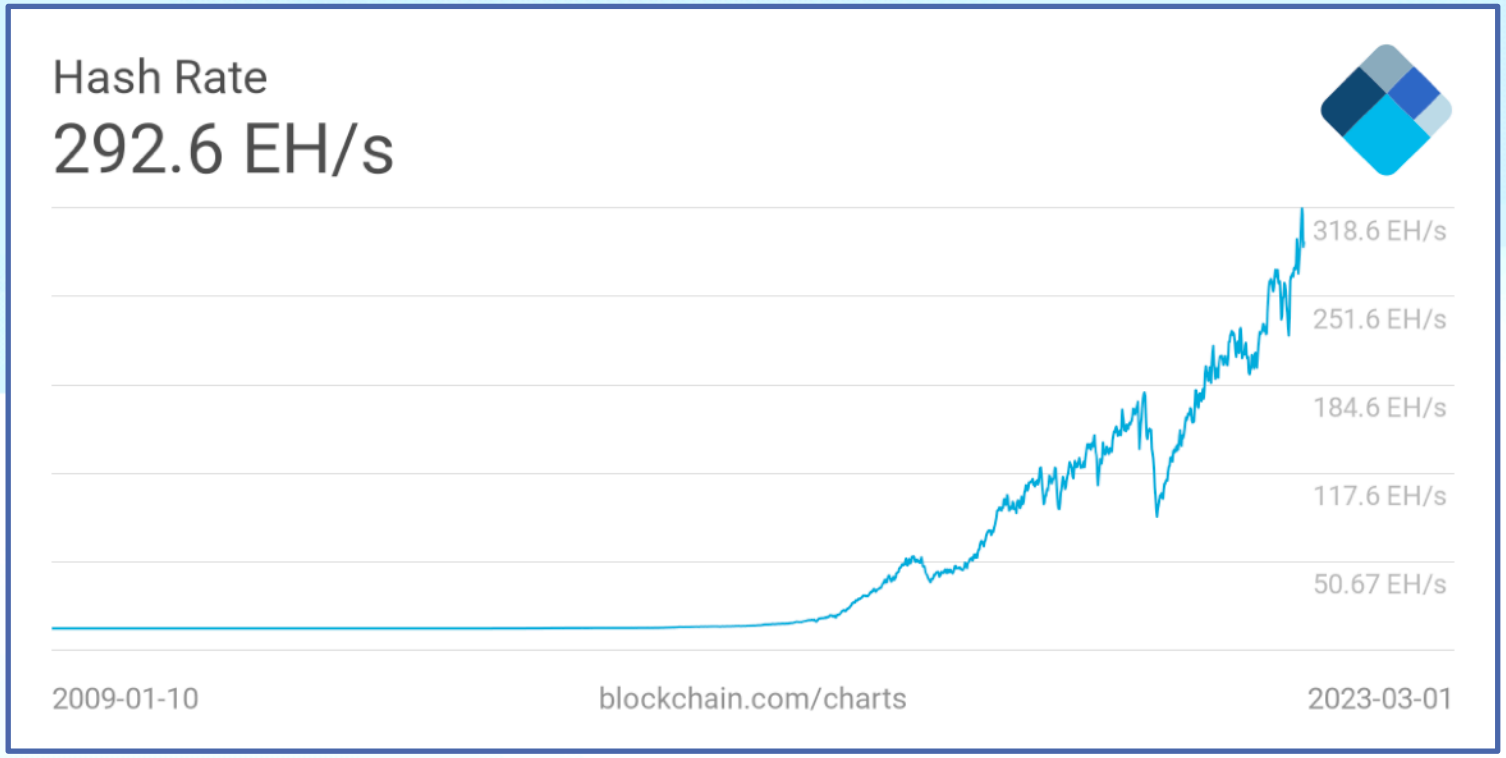
Every two weeks, compute:

```
next_difficulty= previous_difficulty *
                 (2 weeks)/(time to mine last 2016 blocks)
```



Expected number of blocks in 2 weeks at 10 minutes/block

Mining difficulty over time

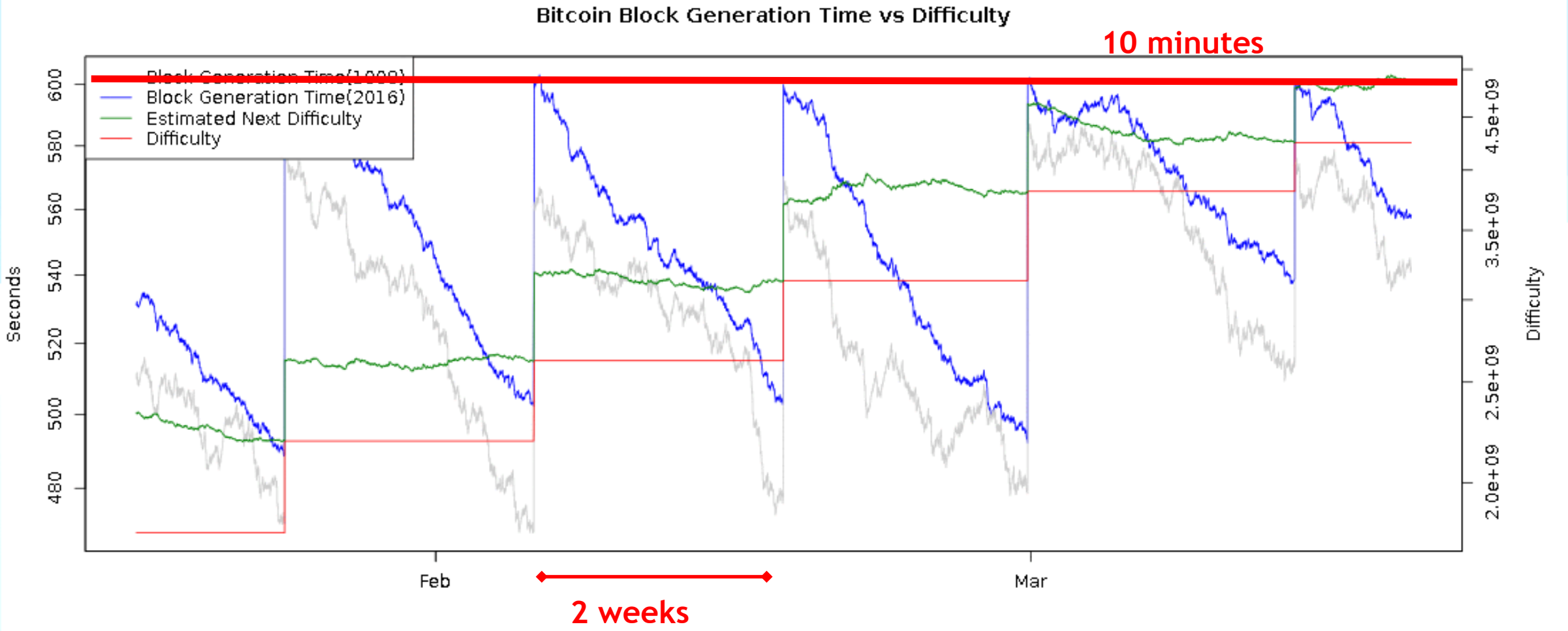


As of September 2024:
Hash Rate: 642-653 exahashes per second (EH/s)

Hash difficulty: 89.5 trillion (T) hashes

https://api.blockchain.info/charts/preview/hash-rate.png?timespan=all&h=600&w=1200&daysAverageString=7D

Time to find a block



bitcoinwisdom.com

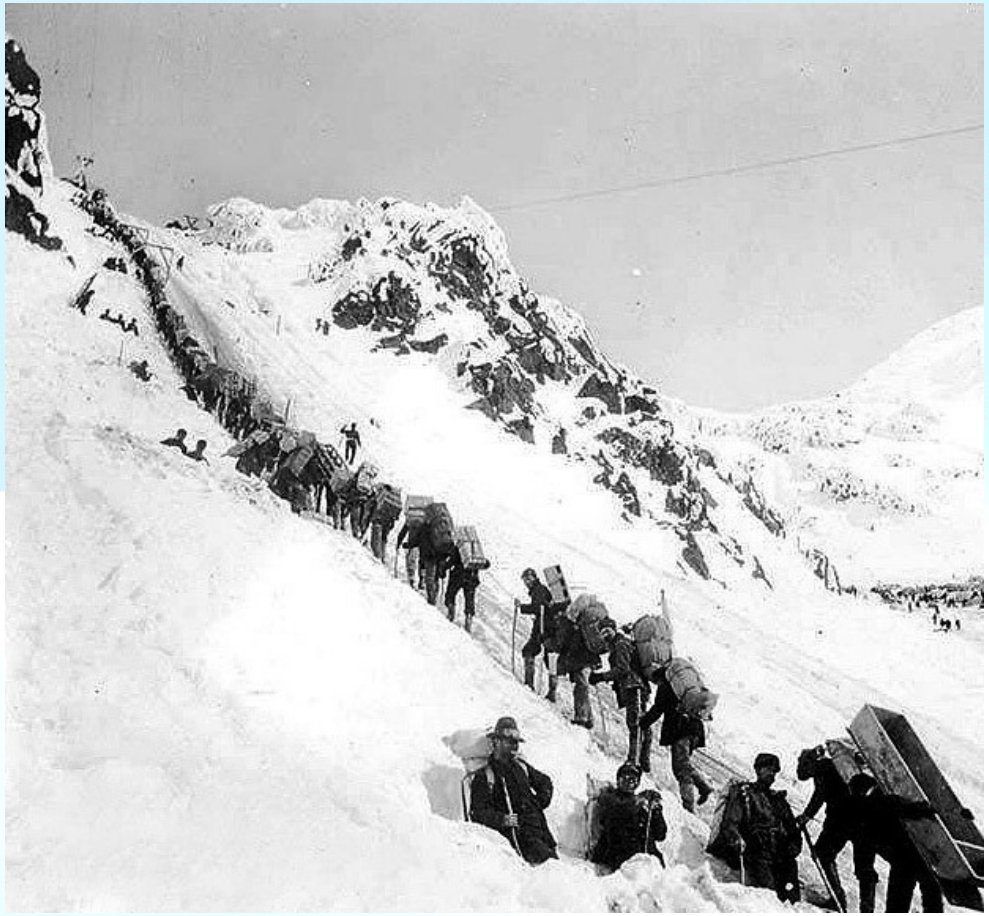
Bitcoin Mining Hardware

Image by macrovector on Freepik

Slides based on Bitcoin and Cryptocurrency Technologies: http://bitcoinbook.cs.princeton.edu/

CBS

So you want to be a miner?



Gold miners ascending the Chilkoot pass

Klondike gold rush of 1898

https://en.wikipedia.org/wiki/Klondike_Gold_Rush

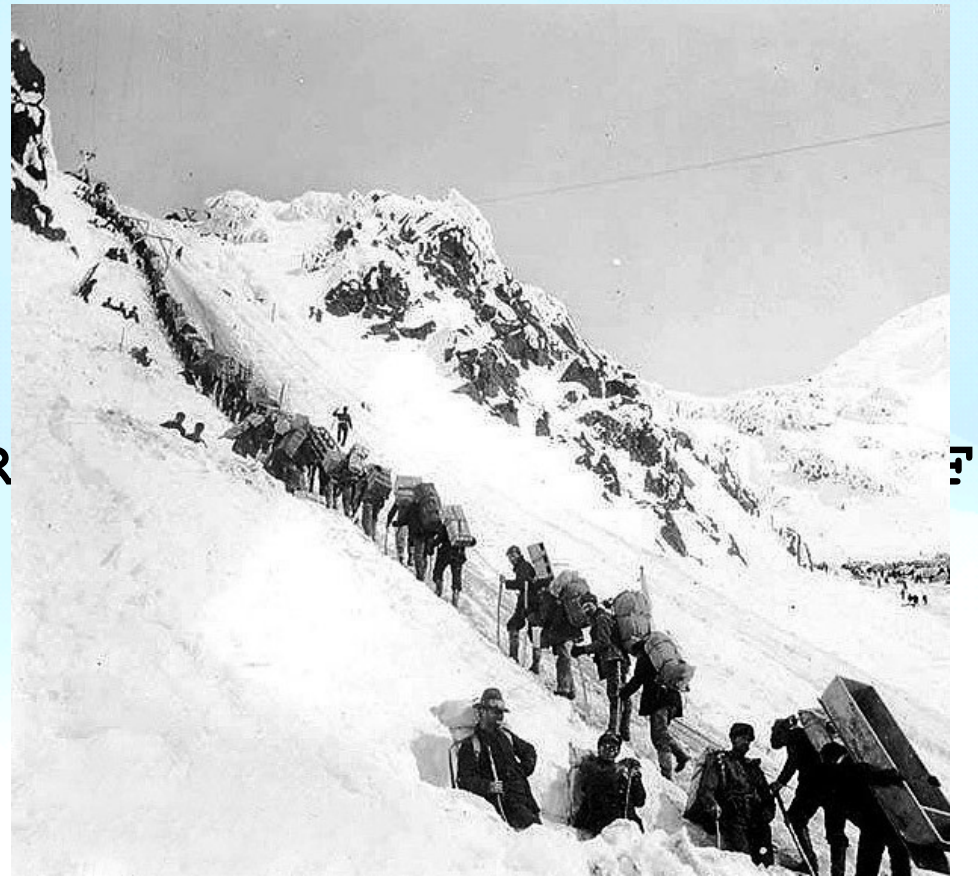
SHA-256

- General purpose hash function
  - Part of SHA-2 family: SHA-224,SHA-384,SHA-512
- Published in 2001
- Designed by the NSA
- Remains unbroken cryptographically
  - Weaknesses known
- SHA-3 (replacement) under standardization

CPU mining

```
while (1){
    HDR[kNoncePos]++;
    IF (SHA256(SHA256(HDR                    FICULTY)
        return;
}
```

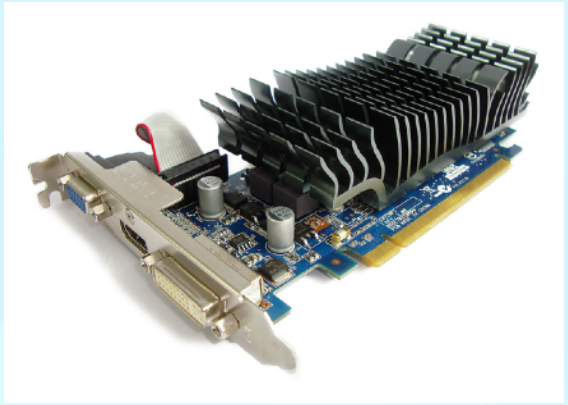
two hashes



Throughput on a high-end PC = 10-**20 MHz** ≈ 2^{24}

139,461 years to find a block today!

GPU mining



- GPUs designed for high-performance graphics
  - high parallelism
  - high throughput
- First used for Bitcoin ca. October 2010
- Implemented in OpenCL
  - Later: hacks for specific cards

GPU mining advantages

- easily available, easy to set up
- parallel ALUs
- bit-specific instructions
- can drive many from 1 CPU
- can overclock!

Source: LeonardH, cryptocurrencies talk.com

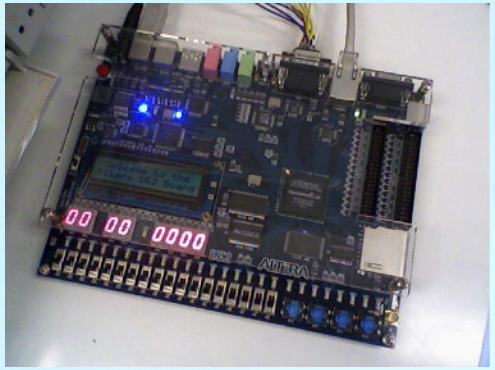
GPU mining disadvantages

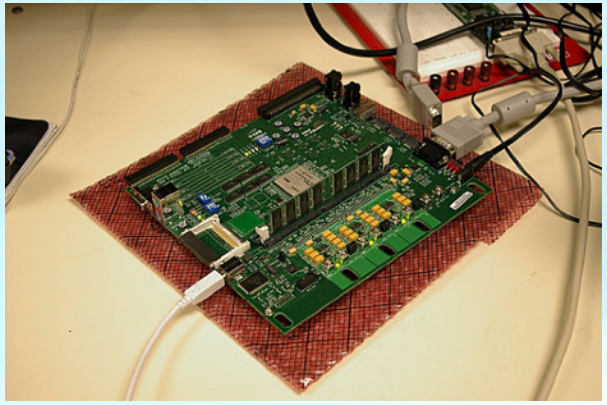
- poor utilization of hardware
- poor cooling
- large power draw
- few boards to hold multiple GPUs

Throughput on a good card = 20-**200 MHz** ≈ 2^{27}

≈**173 years** to find a block w/100 cards!

FPGA mining





- **F**ield **P**rogrammable **G**ate **A**rea
- First used for Bitcoin ca. June 2011
- Implemented in Verilog

FPGA mining advantages

- higher performance than GPUs
  - excellent performance on bitwise operations
- better cooling
- extensive customisation, optimisation

Bob Buskirk, thinkcomputers.org

FPGA mining disadvantages

- higher power draw than GPUs designed for
  - frequent malfunctions, errors
- poor optimization of 32-bit adds
- fewer hobbyists with sufficient expertise
- more expensive than GPUs
- marginal performance/cost advantage over GPUs

Throughput on a good card = 100-**1000 MHz** ≈ 2^{30}

25 years to find a block w/100 boards!

Bitcoin ASICs

TerraMiner™ IV – 2TH/s Networked ASIC Miner

$5,999

Shipping June 2014

300 GH Bitcoin Mining Card

The Monarch BPU 300 C

$1,497.00

Qty: 1 ADD TO CART

Pre-Order Terms: This is a pre-order. 28nm ASIC bitcoin mining hardware products are shipped according to placement in the order queue, and delivery may take 3 months or more after order. All sales are final.

THE LEOPARD

DETAILS :

- **2,5 TH/s**
- Dimensions: 15“ x 13.3“ x 13.7“ (38cm x 34cm x 35cm)
- 28nm ASIC technology
- Silent Cooling
- In-built WiFi Connection (without Antenna)
- Less than 750 watt (0.3 per GH)
- 1 Year Guarantee

- $ 5.800

COMES WITH :

1. Power Supply
2. Free Remote Power Outlet & Smartphone App
3. Free User Guide
4. Free Personal Assistance for Setup

SHIPPING :

- Worldwide, Express
- Included in the price
- Available: 100 Units: Shipping April (Week 3)

Bitcoin ASICs

- special purpose
  - approaching known limits on feature sizes
  - less than 10x performance improvement expected
- designed to be run constantly for life
- require significant expertise, long lead-times
- perhaps the fastest chip development ever!

Case study: TerraMiner IV

- First shipped Jan 2014
- 2 TH/s
- Cost: US$6,000

Still, **14 months** to find a block!

Professional mining centers

Needs:

- cheap power
- good network
- cool climate

BitFury mining center, Republic of Georgia

Video about mining centre:
https://www.youtube.com/watch?v=4ekOcDG2D8E

Evolution of mining

CPU

GPU

FPGA

ASIC

gold pan

sluice box

placer mining

pit mining

How much is a MW?

Tehri Hydropower – 2,400MW

Three Gorges Dam = 10,000 MW
typical hydro plant ≈ 1,000 MW

Kashiwazaki-Kariwa
nuclear power plant = 7,000 MW
typical nuclear plant ≈ 4,000 MW

major coal-fired plant ≈ 2,000 MW

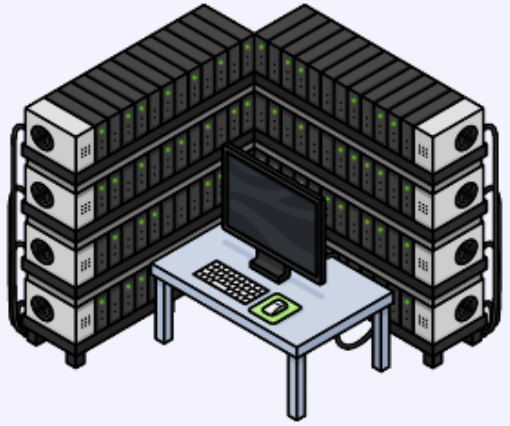
As of 2021, Bitcoin mining consumes 91 Terawatt Hours ~ 10 388 MW

Limitations of Blockchain: **Energy Consumption**

In 2009, you could mine one Bitcoin using a setup like this in your living room.

Amount of household electricity required to mine one coin: **a few seconds' worth**. Bitcoin's value: **basically nothing**.

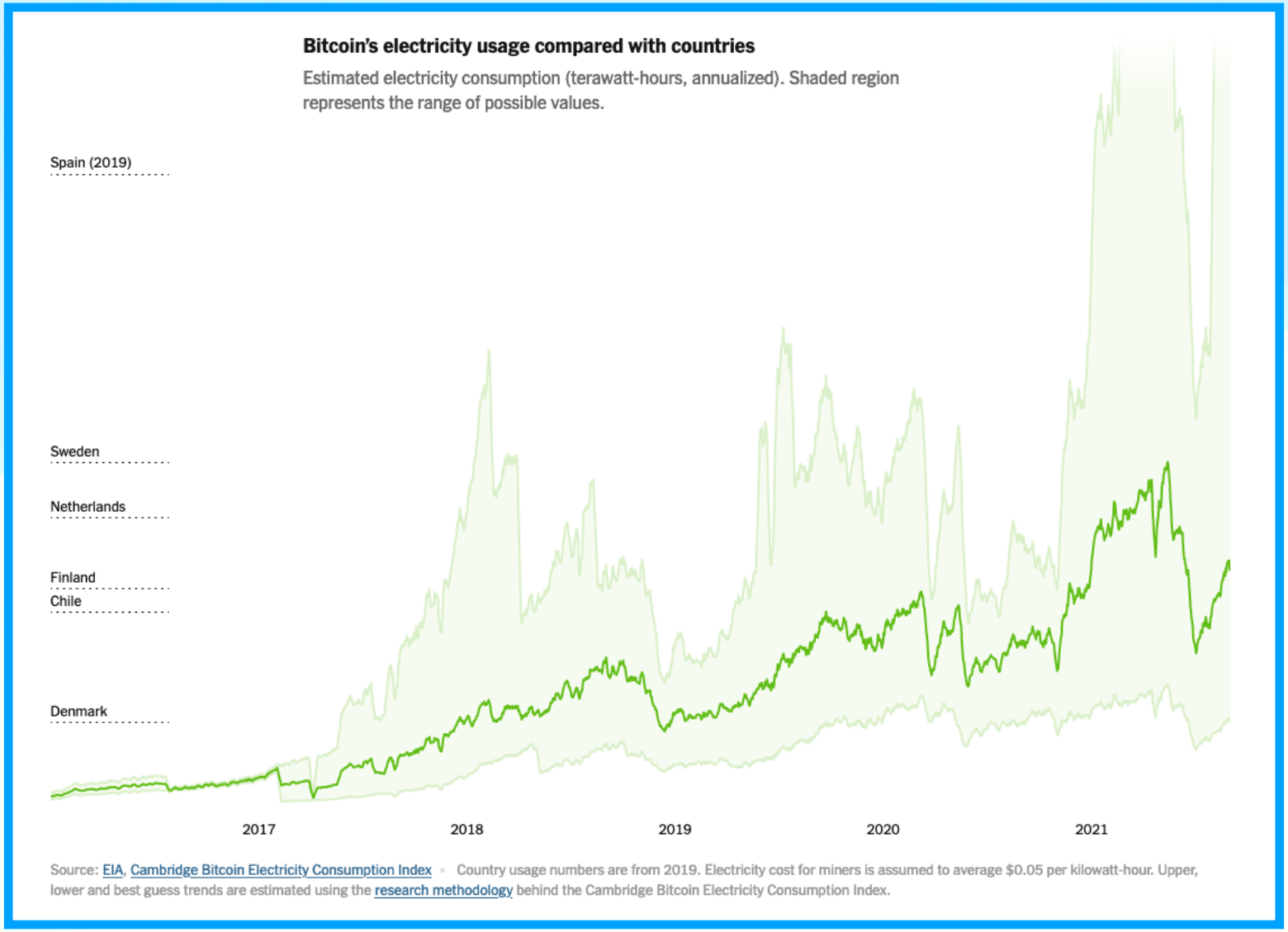
Today, you'd need a room full of specialized machines, each costing thousands of dollars.



Amount of household electricity required: **9 years' worth**. (Put in terms of a typical home electricity bill: **about $12,500**.) Value of one Bitcoin today: **about $50,000**.

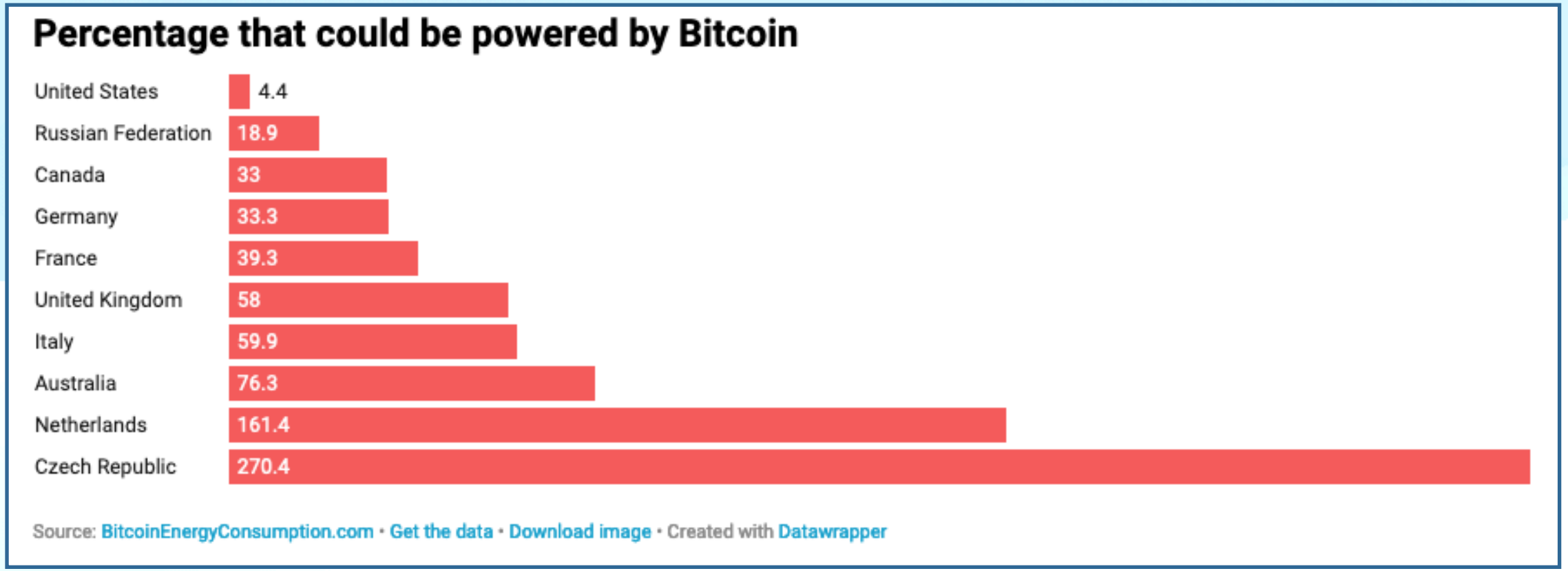
https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html

Limitations of Blockchain: **Energy Consumption**



https://www.nytimes.com/interactive/2021/09/03/climate/bitcoin-carbon-footprint-electricity.html

Limitations of Blockchain: **Energy Consumption**



https://digiconomist.net/bitcoin-energy-consumption

All payment systems require energy

Mining Pools

Image by macrovector on Freepik

Slides based on
1) Bitcoin and Cryptocurrency Technologies: http://bitcoinbook.cs.princeton.edu/
2) Antonopoulos, A. M. (2014). Mastering Bitcoin: unlocking digital cryptocurrencies. " O'Reilly Media, Inc.".

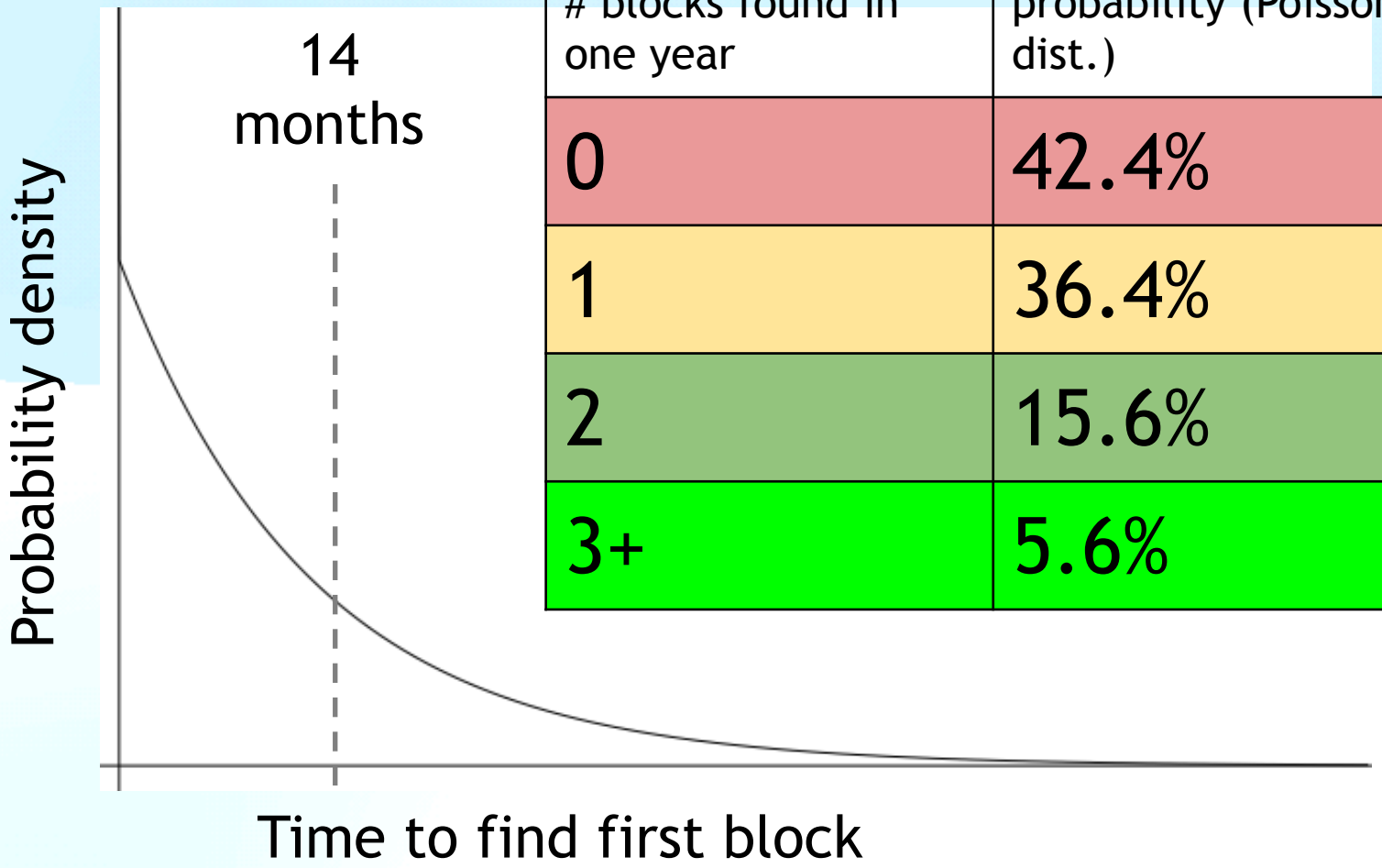
CBS

Economics of being a small miner

TerraMiner IV

- Cost: ≈US$6,000
- Expected time to find a block: ≈14 months
- Expected revenue: ≈$1,000/month

Mining uncertainty



# blocks found in one year	probability (Poisson dist.)
0	42.4%
1	36.4%
2	15.6%
3+	5.6%

Idea: could small miners pool risk?

Mining pools

- **Goal:** pool participants all attempt to mine a block with the same coinbase recipient
  - send money to key owned by pool manager
- Distribute revenues to members based on how much work they have performed
  - minus a cut for pool manager

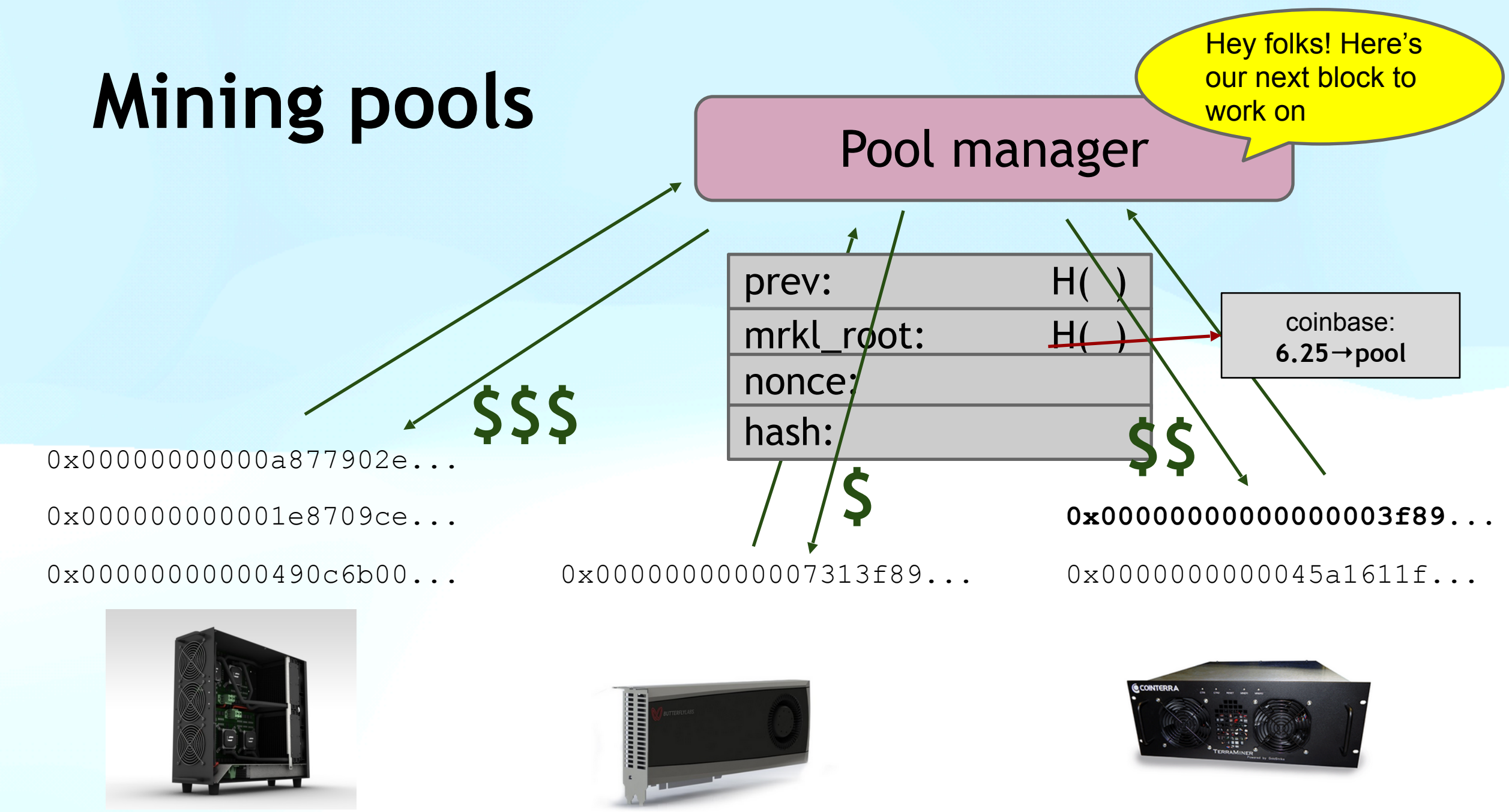
How do we know how much work members perform?

Mining shares

Idea: prove work with “near-valid blocks” (shares)

```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
0000000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
009048813377 9E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
0000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E777613845 6181FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

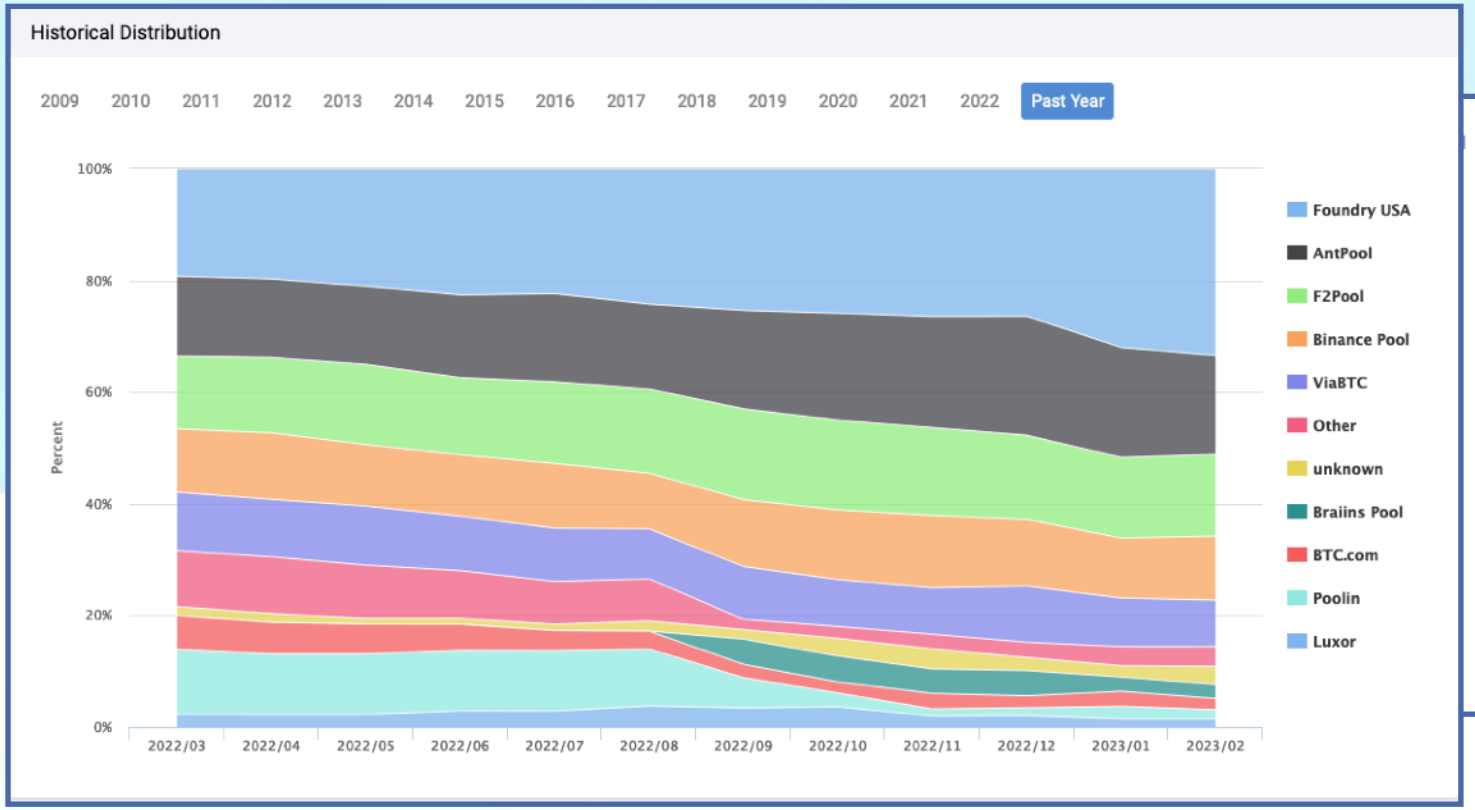
Mining pools

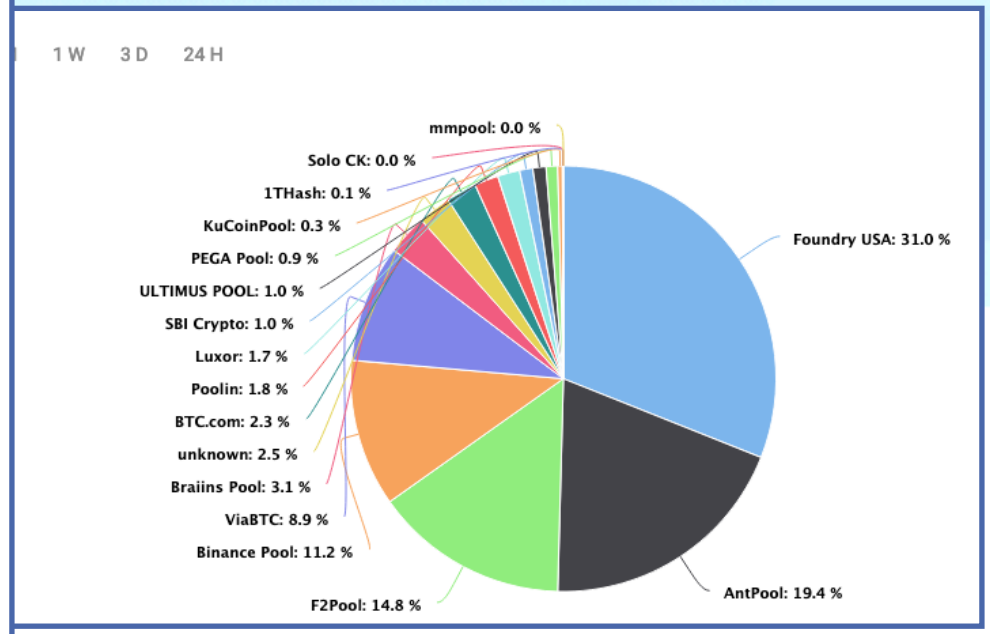


Mining pool variations

- **Pay per share:** flat reward per share
  - Typically minus a significant fee
  - What if miners never send in valid blocks?
- **Proportional:** typically since last block
  - Lower risk for pool manager
  - More work to verify
- **“Luke-jr” approach:** no management fee
  - Miners can only get paid out in whole BTC
  - Pool owner keeps spread

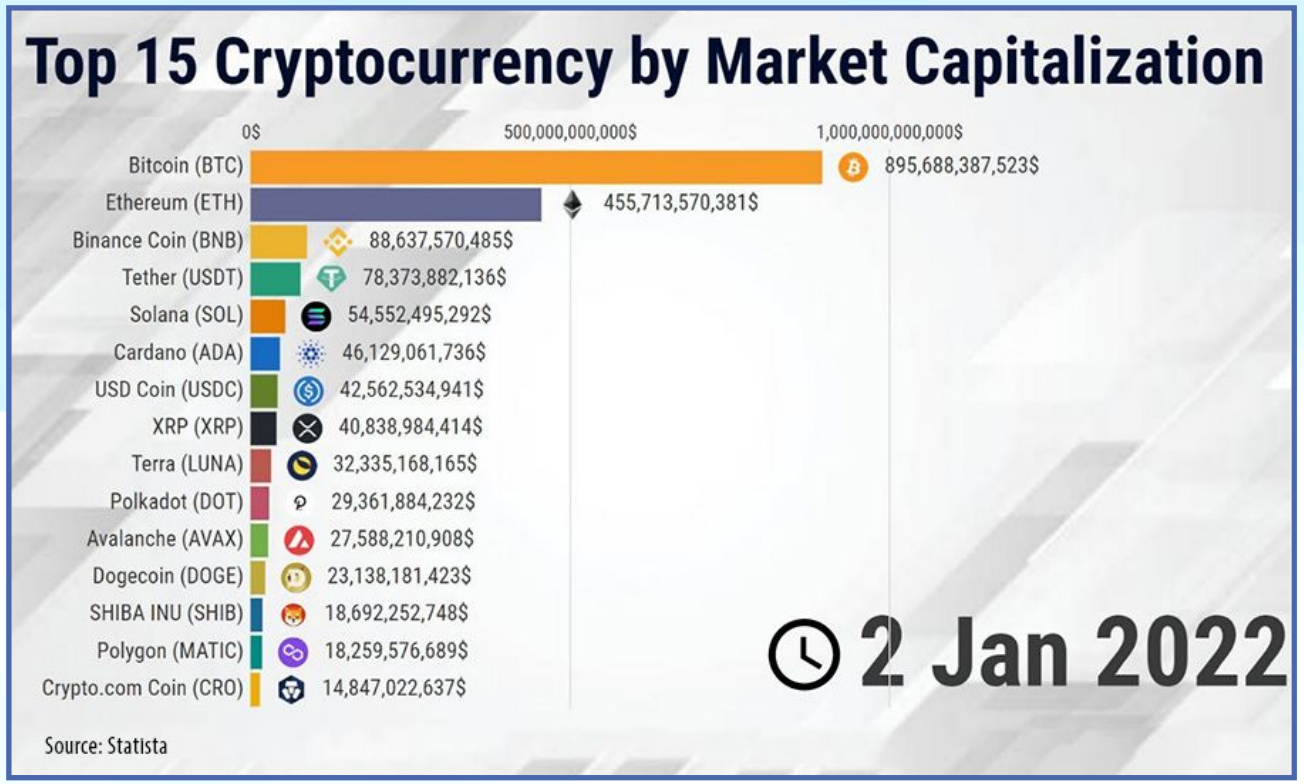
Mining pools (as of March 2023)

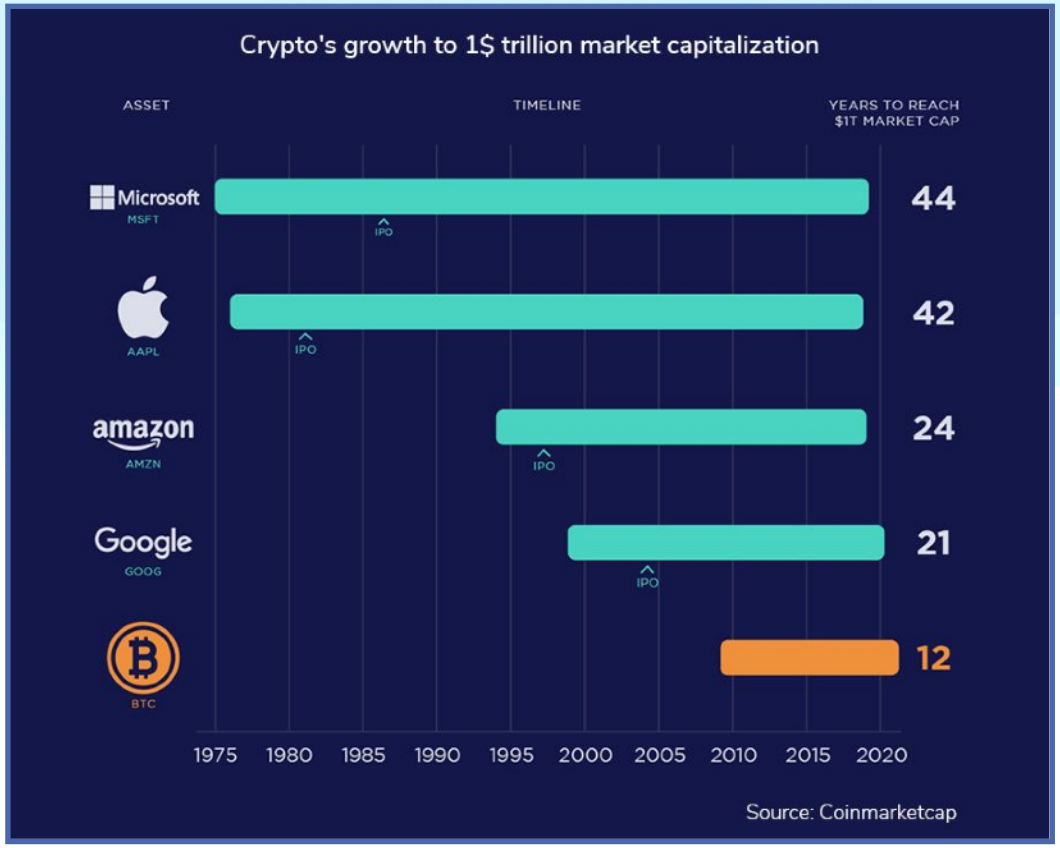




https://btc.com/stats/pool?pool_mode=month3

Cryptocurrency Market Cap





https://www.consultancy-me.com/news/4692/determining-the-real-market-capitalization-of-crypto-assets

Bitcoin Mining

BITCOIN WHITEBOARD TUESDAY

BITCOIN MINING

WHAT IS IT AND IS IT STILL PROFITABLE??

https://www.youtube.com/watch?v=BODyqM-V71E

Thank you!

Raghava Mukkamala

rrm.digi@cbs.dk

https://www.cbs.dk/staff/rrmdigi

https://raghavamukkamala.github.io/

https://cbsbda.github.io/