Bitcoin Mining 101

Prepared by Blockware Intelligence

Table of Contents

- What is Bitcoin?

- What is the blockchain?

- What is Proof of Work?

- What is a valid block?

- What is hashrate?

- What is the block reward?

- What is the difficulty adjustment?

- What is a Bitcoin mining rig?

- How large is the Bitcoin mining market?

- What is the mining business model?

- How does mining balance energy grids?

- Does mining prevent methane flaring?

What is Bitcoin?

Bitcoin is a peer to peer electronic cash system, and the Bitcoin network is composed of three key participants.

Users: Send, receive, and hold BTC.

Miners: Add batches of new transactions called 'blocks', to the ledger of all transactions, the 'blockchain'.

Nodes: Validate all blocks with a self-imposed and universally agreed upon ruleset.

Users   Miners   Nodes

Miners and users can inexpensively and quickly run a Bitcoin full node to validate transactions. Because anyone can easily run a full node, changes to Bitcoin must be backward-compatible or gain full network consensus among all stakeholders. This makes Bitcoin resistant to major changes and reduces its future uncertainty.

Sources: Bitcoin Whitepaper

What is the blockchain?

The Bitcoin 'blockchain' is a digitally distributed, decentralized, and immutable public ledger.

A 'block' refers to a batch of transactions.

Each block is 'chained' to the previous block. Changing the data inside of a single block will change all subsequent blocks.

Anybody running a node can audit the Bitcoin blockchain, ensuring each transaction and block are valid to the rules set by the software the user runs.
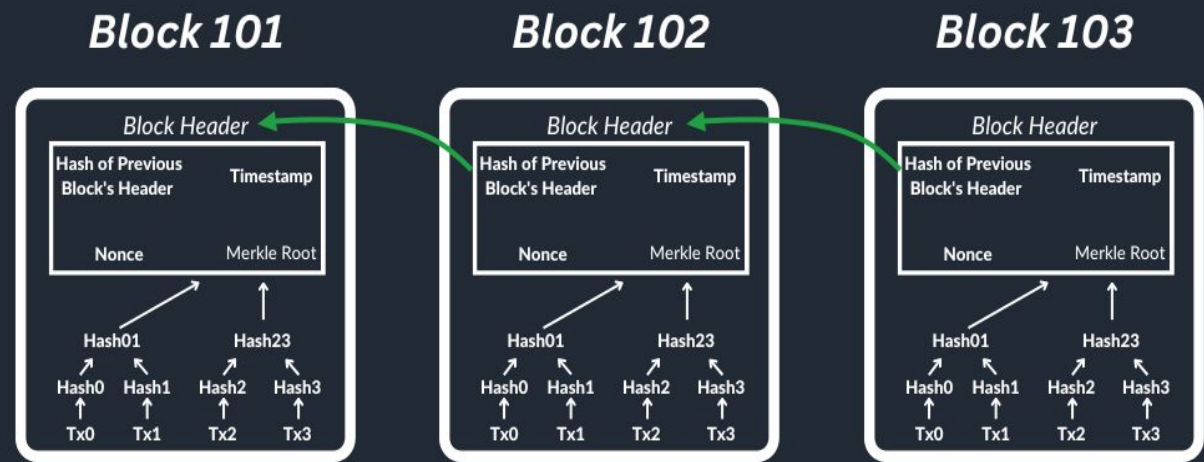
Blocks in the blockchain connect to each other by referencing a hash of the previous blocks header.
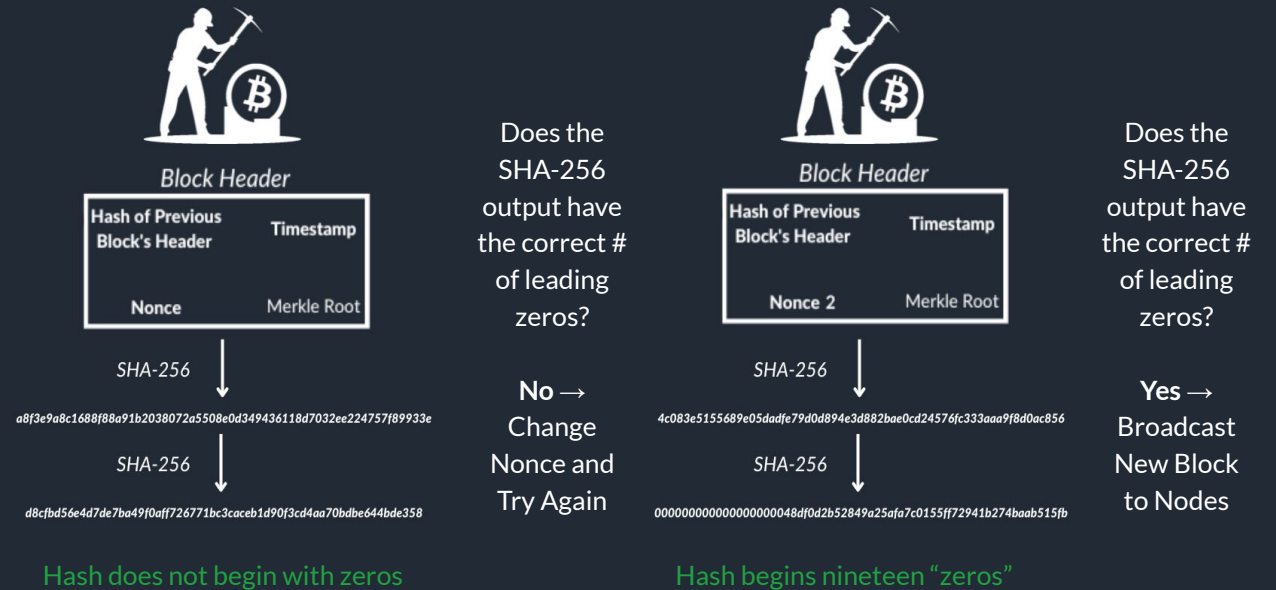
Sources: Bitcoin Whitepaper

What is Proof of Work?

Proof of Work (PoW) is a form of cryptographic proof in which one party (the prover) proves to others (the verifiers) that a certain amount of a specific computational effort has been expended.[2]

"Cryptographic proof" comes from the SHA-256 hashing algorithm: a one-way function that converts text input into a unique output of 256 bits (64 characters).

To add a block to the blockchain the network requires the SHA-256 output contain a certain number of zeros at the beginning of the output.

Miners that find a valid hash output are proving that they used a large amount of computational power (proof of work), because the only way to find a valid hash, containing the required number of leading zeros, is to guess and check many times.

Block Header

Hash of Previous Block's Header	Timestamp
Nonce	Merkle Root

SHA-256

a8f3e9a8c1688f88a91b2038072a5508e0d349436118d7032ee224757f89933e

SHA-256

d8cfbd56e4d7de7ba49f0aff726771bc3caceb1d90f3cd4aa70bdbe644bde358

Hash does not begin with zeros

Does the SHA-256 output have the correct # of leading zeros?

No → Change Nonce and Try Again

Block Header

Hash of Previous Block's Header	Timestamp
Nonce 2	Merkle Root

SHA-256

4c083e5155689e05dadfe79d0d894e3d882bae0cd24576fc333aaa9f8d0ac856

SHA-256

0000000000000000000048df0d2b52849a25afa7c0155ff72941b274baab515fb

Hash begins nineteen "zeros"

Does the SHA-256 output have the correct # of leading zeros?

Yes → Broadcast New Block to Nodes

Sources: Bitcoin Whitepaper, Lachtar, Elkhail, Bacha and Malik

What is a valid block?

Blocks that miners produce must meet the following six requirements to be accepted by nodes.

1. All transactions inside the block are valid (no double spending).

2. The miner subsidy is not greater than the maximum allowable amount in accordance with the BTC halving schedule.

3. The SHA-256 hash output contains the minimum number of required leading zeros (PoW).

4. Block size does not exceed 4,000,000 weight units (~4MB).

5. Block data is structured with correct syntax.

6. The block timestamp is less than two hours in the future (allows for time errors).
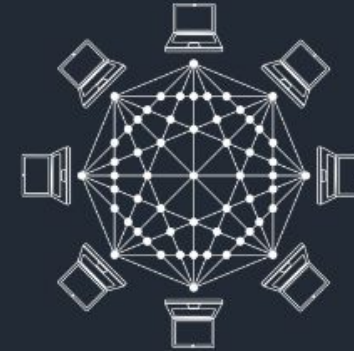
Does the broadcasted block meet all requirements?

No   Yes

Ignore   Add to chain

If multiple valid blocks are broadcasted, Nodes accept the longest chain with the most proof of work as the correct chain.

Sources: Bitcoin Whitepaper

What is hashrate?

Hashrate is the unit of measurement for the computational power being utilized by miners on the Bitcoin network. This can refer to the network as a whole or the hashing ability of an individual mining rig (ASIC.)

The hashrate of the Bitcoin network, the total number of hashes generated per second by all Bitcoin miners, as of January 17th, 2023, is roughly ~268 EH/s. 268 EH/s = 268 'Exahash' per second = 1 Quintillion Hashes per second.

Significant increases in hashrate tend to occur 6-18 months after Bitcoin price bull runs. When the price of Bitcoin increases significantly, so does mining profitability. Higher profits entice new miners to enter the market, as well as enticing existing miners to build out more infrastructure.

BTC: Price, Hashrate (14D Moving Avg.)

BLOCKWARE SOLUTIONS

Source: Glassnode

Due to day-to-day variability, the Bitcoin network hashrate tends to be measured using a 14-day or 30-day moving average.

Sources: Glassnode

What is the block reward?

Miners earn a reward for every block mined. The block reward consists of two parts.

1. Block Subsidy
2. Transaction Fees

The block subsidy is new BTC entering into circulation. The current block subsidy is 6.25 BTC per block. Every 210,000 blocks (approximately every 4 years) the block subsidy is cut in half. At block 6,930,000, in the year 2140, the block subsidy will decrease from 1 sat (1 / 100,000,000th of a BTC) to zero sats.

Each transaction on-chain pays a fee to the miner that is determined entirely by free market forces. When demand is high (bull market), those wishing to have their transaction included in a block will need to pay a higher fee in order to incentivize miners to include their transaction instead of someone else's.

Year	Block Number	BTC Block Subsidy
2009	0	50
2012	210000	25
2016	420000	12.5
2020	630000	6.25
2024	840000	3.125
2028	1050000	1.5625
2032	1260000	0.78125
2036	1470000	0.390625
2040	1680000	0.1953125
2044	1890000	0.09765625
2048	2100000	0.04882812
2052	2310000	0.02441406
2056	2520000	0.01220703
2060	2730000	0.00610351
2064	2940000	0.00305175
2068	3150000	0.00152587
2072	3360000	0.00076293
2076	3570000	0.00038146
2080	3780000	0.00019073
2084	3990000	0.00009536
2088	4200000	0.00004768
2092	4410000	0.00002384
2096	4620000	0.0000192
2100	4830000	0.00000596
2104	5040000	0.00000298
2108	5250000	0.00000149
2112	5460000	0.00000074
2116	5670000	0.00000037
2120	5880000	0.00000018
2124	6090000	0.00000009
2128	6300000	0.00000004
2132	6510000	0.00000002
2136	6720000	0.00000001
2140	6930000	0

What is the difficulty adjustment?

The difficulty adjustment is a mechanism ensuring blocks are mined every ~10 minutes, regardless of how many miners are online.

Difficulty adjusts every 2,016 blocks, which is approximately 14 days. If blocks are mined faster than expected, difficulty will increase, and vice versa for a decrease.

Difficulty determines a miner's expected BTC rewards per TH/s. The greater the difficulty, the lower the mining rewards per TH/s.

BLOCKWARE SOLUTIONS

Hashrate (14D Moving Avg.), **Difficulty**

Source: Glassnode
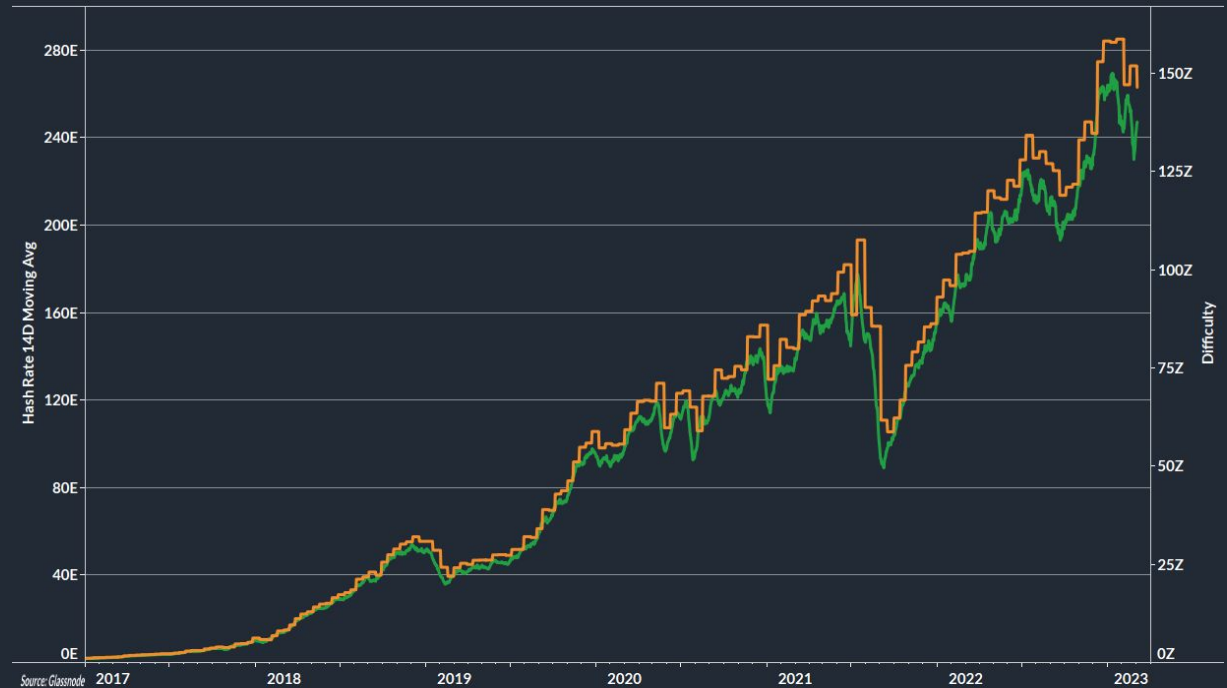
By increasing or decreasing the required number of leading zeros for the proof of work, difficulty is adjusted 1:1 with hashrate.

Sources: Bitcoin Whitepaper, Glassnode

What is a mining rig?

Bitcoin mining rigs are specialized, energy dense computers called ASICs (Application Specific Integrated Circuits) that are designed for the sole purpose of mining Bitcoin as efficiently as possible.

The market price of an ASIC is strongly correlated with the price of Bitcoin. Other factors determining the market price of an ASIC are the number of hashes the ASIC can produce per second, and the number of energy units consumed to produce each hash.

How large is the Bitcoin mining market?

The industry is rapidly growing as evidenced by the surge in network hashrate as well as the number of publicly traded mining companies. As it stands, Bitcoin mining is nearly an $8 billion per-year industry.

The network hashrate has nearly tripled in the past three years and the number of publicly traded mining companies has eclipsed twenty, up from just a handful in years prior.

$7.68 Billion
Annual Bitcoin mining revenue. 328,500 new BTC mined each year * $23,400 per BTC

1.7 Million
BTC left to be mined between now and the year 2140.

$4.17 Billion
Combined market cap of the top 17 largest publicly traded Bitcoin mining companies.

What is the mining business model?

There are multiple industry segments in which Bitcoin miners generate revenue.

ASIC Manufacturing: Research & development on new ASIC chips. Production and wholesale distribution of ASICs.

Self-Mining: Mine BTC using your own ASICs. Profit is the difference between the price of BTC and the cost of production

Hosted-Mining: Operate and maintain someone else's ASICs for a fee.

Hardware Sales: Wholesale purchasing from ASIC manufacturers and sell to miners at a higher price.

Grid Balancing Service: Receive payment in cash or energy credits from energy suppliers in exchange for curtailing power use during times of peak demand.

ASIC Manufacturing	Self Mining	Hosted Mining	Hardware Procurement	Grid Balancing
BITMAIN	BLOCKWARE SOLUTIONS	BLOCKWARE SOLUTIONS	BLOCKWARE SOLUTIONS	HIVE
whatsminer	MARATHON	cryptech.	cryptech.	R
AvalonMiner	HUT 8	CORE SCIENTIFIC	RIVER FINANCIAL	MARATHON
KCI miner	cryptech.	RIVER FINANCIAL	Luxor	Bitfarms
MicroBT 比特微	R	Luxor		
	CORE SCIENTIFIC			argo

What is the mining business model?

Bitcoin mining profitability is a function of:

1. BTC Price
2. Bitcoin Network Difficulty
3. ASIC Model Efficiency
4. Energy Cost

Considering a miner has no control over the BTC price and network difficulty, using the most efficient ASICs with the cheapest available power source is how a Bitcoin miner can maximize their profitability.

Slight changes in the electricity rate or ASIC efficiency have a huge impact on a miner's profitability. At current price and difficulty, an S19 XP can mine profitably even with an electricity rate as high as 9¢/kWh. An S9 would require an electricity rate of 2¢/kWh, over 4.5x cheaper, to produce a Bitcoin profitably.

Layer	Eletricity Rate ($/kWh)	S9 Shutoff BTC Breakeven Price	S17 Shutoff BTC Breakeven Price	S19 Shutoff BTC Breakeven Price	S19XP Shutoff BTC Breakeven Price
1	$0.01	$7,258.13	$3,199.50	$2,168.55	$1,528.65
2	$0.02	$14,516.25	$6,399.00	$4,337.10	$3,057.30
3	$0.03	$21,774.38	$9,598.50	$6,505.65	$4,585.95
4	$0.04	$29,032.50	$12,798.00	$8,674.20	$6,114.60
5	$0.05	$36,290.63	$15,997.50	$10,842.75	$7,643.25
6	$0.06	$43,548.75	$19,197.00	$13,011.30	$9,171.90
7	$0.07	$50,806.88	$22,396.50	$15,179.85	$10,700.55
8	$0.08	$58,065.00	$25,596.00	$17,348.40	$12,229.20
9	$0.09	$65,323.13	$28,795.50	$19,516.95	$13,757.85

This table shows how much it costs to produce 1 BTC, the 'breakeven' price, for various ASIC models at different electricity rates. Breakeven prices were calculated using data from January 17th 2023; with the price of Bitcoin at $21,330 and hashprice at $0.072. Red text indicates it would be unprofitable to mine with the specified ASIC at the corresponding electricity rate.

What is the mining business model?

Mining can be performed anywhere with an internet connection, as such, miners gravitate towards remote regions that contain cheap and abundant energy.
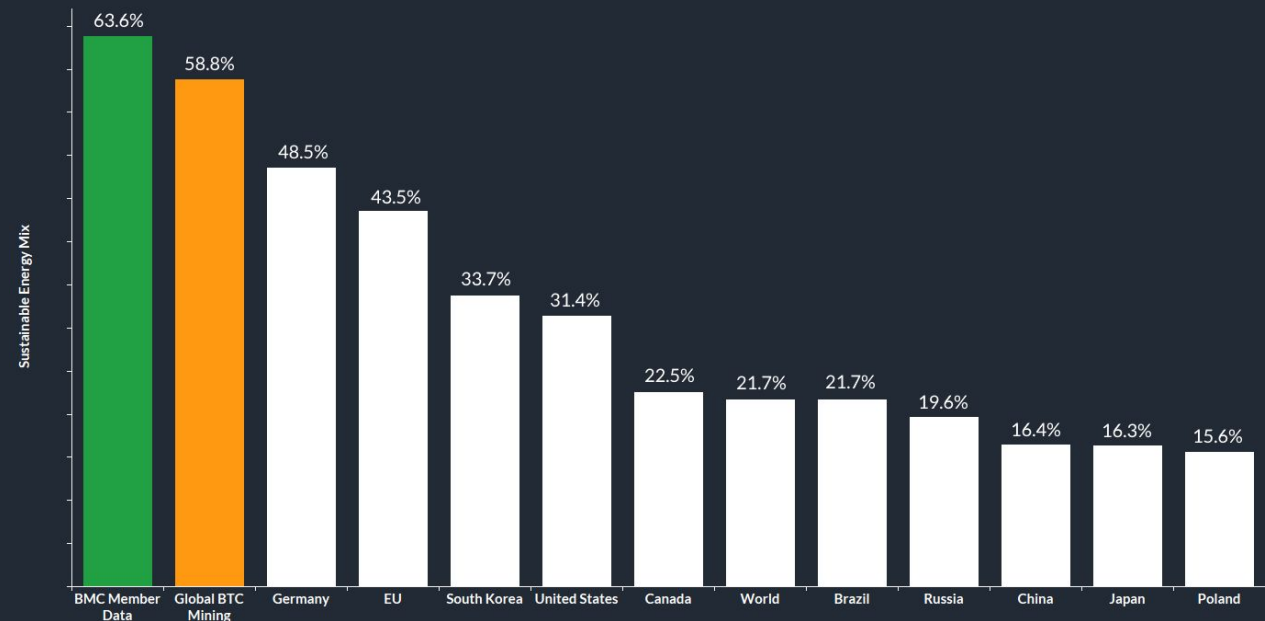
The United States has become a favorite destination for Bitcoin miners as it has stable energy prices, lower inflation, political stability and more secure property rights.

There is now a much stronger financial incentive for energy companies to build sustainable energy infrastructure, because they know they can rely on Bitcoin miners to purchase that energy if nobody else will. The desire of miners to consume energy with the lowest cost has driven a 58% sustainable energy mix for miners.

BLOCKWARE SOLUTIONS

Sustainable Power Mix: Bitcoin Mining vs Countries (% of TWh)
Source: Bitcoin Mining Council

Sustainable Energy Mix

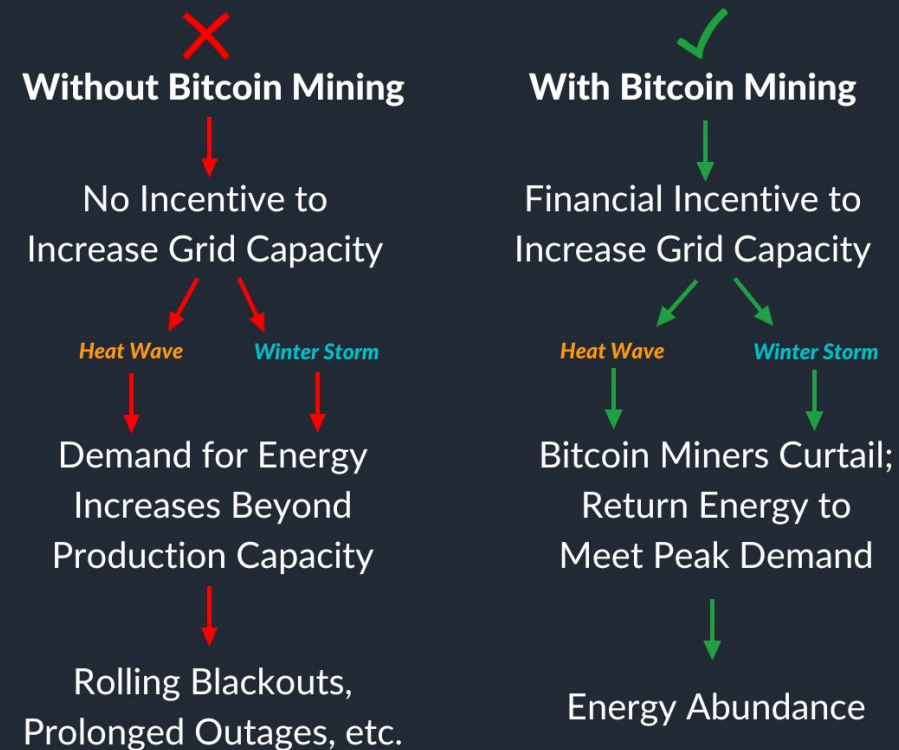| Category	Value
BMC Member Data	63.6%
Global BTC Mining	58.8%
Germany	48.5%
EU	43.5%
South Korea	33.7%
United States	31.4%
Canada	22.5%
World	21.7%
Brazil	21.7%
Russia	19.6%
China	16.4%
Japan	16.3%
Poland	15.6%

58.8% of the energy consumed by Bitcoin miners is produced by sustainable power sources. This is a greater percentage than all nations on earth.

Sources: Bitcoin Mining Council

How does mining balance energy grids?

Bitcoin miners balance energy grids, making them more resilient during times of stress, as well as lowering the marginal cost of production, decreasing the price for other consumers.

Bitcoin miners are energy buyers of last resort. Energy companies now have a customer to whom they can sell large amounts of energy to all year long; creating an economically sound path for building larger energy grids. Unlike other 24/7/365 energy consumers, namely hospitals, Bitcoin miners have the flexibility to turn off instantly during times of peak demand; giving energy back to the grid.

Without Bitcoin Mining

No Incentive to Increase Grid Capacity

Heat Wave   *Winter Storm*

Demand for Energy Increases Beyond Production Capacity

Rolling Blackouts, Prolonged Outages, etc.

With Bitcoin Mining

Financial Incentive to Increase Grid Capacity

Heat Wave   *Winter Storm*

Bitcoin Miners Curtail; Return Energy to Meet Peak Demand

Energy Abundance

How does mining balance energy grids?

Bitcoin miners are prime candidates for demand response programs. These are programs in which energy companies offer financial incentives to consumers if said consumers elect to reduce their consumption during peak demand periods.

Beyond the financial incentives offered through demand response programs, miners are also incentivized to curtail their operations during peak demand due to the higher associated power costs. As energy demand increases to peak capacity, energy companies are forced to tap into alternative, less-efficient sources, resulting in a higher price for the end consumers.

A marginal change in the price of energy can greatly affect the profitability of Bitcoin mining, as such, miners who engage in "peak avoidance" are likely to be more profitable than those that continue mining during peak demand.
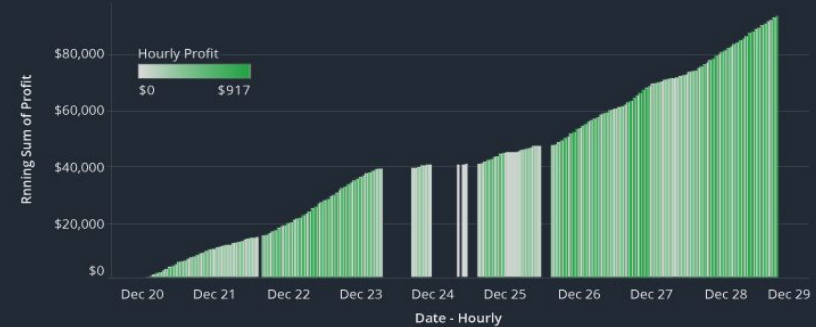
Texas Miners that temporarily halted operations during peak demand in December 2022 were far more profitable than those that continued mining in spite of the increased electricity costs. Data sourced by Mitch Klee and Foreman Mining.

Sources: Foreman Mining, Foreman Mining

Does mining prevent methane flaring?

Over 144 billion cubic meters of gas are flared annually, resulting in the emission of approximately 400 million tons of CO_2.

Bitcoin mining provides a profitable alternative use for this gas that would otherwise be flared. Bitcoin miners are willing to travel to the remote locations where oil is produced and consume large quantities of the stranded energy.

The White House estimates that mining emits ~154 million (+/- 33M) tons of CO_2 annually. This is less than half of the emissions caused by flaring which means Bitcoin mining has the potential to have a net-negative carbon footprint.

During the process of drilling for oil, a buildup of natural gas occurs. It is uneconomical to transport the gas to populated areas where it can be used. As such, it must be disposed, and the safest method of disposal is to burn it into the atmosphere, a process known as flaring.

Sources: whitehouse.gov, worldbank.org

Glossary

ASIC: A specialized computer designed exclusively for the purpose of mining Bitcoin.

Bitcoin: The distributed network consisting of users, miners, and nodes.

bitcoin / BTC: The asset transferred on the Bitcoin network.

Block: A ledger of data (mostly transactions).

Blockchain: A sequential series of blocks.

Block Reward: The BTC rewarded to miners for successful adding a block to the blockchain. Comprised of the block subsidy and transaction fees.

Block Subsidy: New BTC mined into circulation as part of the block reward.

Difficulty: A measure of the computational power required to produce a valid Bitcoin block.

Flaring: Burning of stranded natural gas, built up from oil production, into the atmosphere.

Hash: A string of 64 characters that is the output of inputting data into the SHA-256 algorithm. Each data input has a unique and unpredictable output.

Hashprice: A measure of how much $ an ASIC can expect to earn. This measure is a function of BTC price, difficulty, and the computational power of the machine. $/th/day.

Hashrate: A measure of computational power in terms of SHA-256 hashes produced per second. Used in reference to the Bitcoin network as well as individual mining rigs.

Peak Demand: The time of year in which stress on electrical grids is the greatest. Typically this occurs during the hottest and coldest days of the year.

Transaction Fees: Fees paid by users to miners as part of the Block reward.

BLOCKWARE SOLUTIONS™

✉ Sales@blockwaresolutions.com

✉ blockwaresolutions.com/contact

Blockware Solutions LLC
3800 N. Lamar Blvd.,
Suite 200
Austin, TX 78756

www.blockwaresolutions.com