NYDIG

APRIL 2022

A Primer On **Bitcoin Mining**

Greg Cipolaro
GLOBAL HEAD OF RESEARCH

Ethan Kochav
RESEARCH ANALYST

Executive **Summary**

Mining is an essential function of the Bitcoin network. It is one of the key features that enables Bitcoin to be an open payment network without the need for trust in a central coordinating entity. At a high level, mining is the security function of the network. Mining ensures that transactions reach their destination, funds are safely stored, and tens of thousands of computers around the world stay in sync. Bitcoin mining can be analogized to traditional mining; however, there are many nuances to Bitcoin mining that make it unlike traditional resource extraction. Overextending the metaphor can lead to misunderstandings of the bitcoin mining industry. This primer looks under the hood at Bitcoin mining. We explore how mining works, the industry structure and players, and the drivers of mining's economics.

What is **Bitcoin Mining?**

Bitcoin mining is the act of expanding Bitcoin's digital ledger — called the blockchain — and ensuring that it adheres to prescribed rules. It is performed by specialized actors called miners, who are incentivized for performing this function.

The Bitcoin network consists of tens of thousands of computers around the world, known as nodes. These nodes form a payment network that moves trillions of dollars around the world each year all without coordination from a central entity.

For this all to work, this global web of computers must agree on a common state of the network. That means that all computers must agree on which users, identified publicly by addresses, own which bitcoin balances.

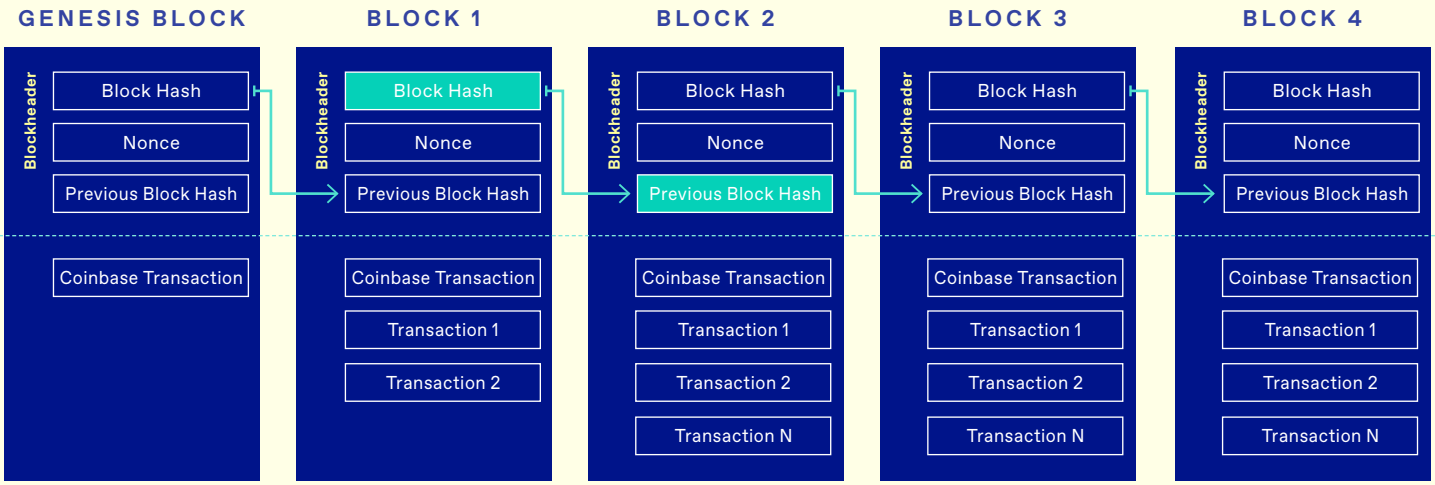
Miners perform this coordination function for the Bitcoin network. In traditional closed payment systems, coordination is achieved by a trusted third party, like a bank or credit card network. However, with the advent of Bitcoin, for the first time, value can be directly and securely transferred without the need for an intermediary. To pull this off, Bitcoin makes use of previously available technologies in the mathematical field of cryptography, using them in a novel manner and adding strong economic incentives. Miners perform the essential security function of aggregating transactions, ensuring that they adhere to the predefined rules of the network, and ordering them into batches called blocks. This effectively timestamps the transaction history of Bitcoin. Miners expend real-world resources in the course of carrying out this security function. Those resources come in the form of electricity consumption and computational resources. For their effort, miners are rewarded with bitcoins.

Why is Bitcoin Mining **Necessary?**

Mining is essential to the security of Bitcoin's network. To fully eliminate the reliance on a trusted third party, Bitcoin needs to prevent funds from being spent by an unauthorized user or being spent by an authorized user more than once. The first issue is solved using **digital signatures,** a cryptographic breakthrough invented in the 1970s. The private-public key pair creates a strong proof of control that allows only the holder of a private key to spend or move bitcoins. However, digital signatures alone are not enough to ensure transaction recipients that the bitcoins they received have not also been sent elsewhere.

To make this guarantee, the network needs to order transactions to confirm that bitcoins have not been previously spent. This issue, known as the "double-spend problem" is solved by **hash-based proof of work.** Originally conceived in 1997 by Adam Back to prevent email spam, hash-based proof of work allows transactions to be ordered into blocks and for the network to achieve agreement on the current state by looking at the longest chain of blocks. As we will go into more detail later, by chaining proofs of work together from block to block, transactions only become reversible if a malicious actor redoes all the preceding proofs of work. And given that the network is constantly making new blocks, it is extremely difficult for any one actor to ever catch up.

Proofs of Work are Chained Together, Making Reversing Previous Transactions Increasingly Difficult



How Does **Mining Work?**

A Deeper Dive into the Blockchain

To understand bitcoin mining, we first need to understand Bitcoin's underlying technology.

The **blockchain** is a shared database that accounts for user balances of bitcoins. Each "block" contains a set of transactions that accounts for the transfers of bitcoins between users, each of which is represented by an alphanumeric string called an **address**. These transactions are published by users across the network to a shared network resource called the **mempool** (memory pool). Transactions are not recognized by the network until after they are added from the mempool to the blockchain. To send bitcoins to an address, the sender must include fees as an incentive to miners to pick their transactions from all the possible ones in the mempool. Blocks have a maximum size so miners select the transactions from the mempool that will deliver them the most revenue, those transactions with the highest fees per block space. They then create a block from these transactions and propagate it across the network to be validated by the nodes. To create a valid block, miners need to show that they have expended effort — literally proof that they have done work — in the form of computation. These proofs are chained together from block to block making it exceedingly difficult for entities to reverse previous transactions. In that sense, proof of work mining secures the network. We describe how this process works in the following section.

How Does Proof of Work Work?

The proof of work mechanism serves two purposes. First, it ensures that each network participant shares the same copy of the blockchain, the dataset that accounts for everyone's balance of bitcoins. Second, it safeguards against funds being spent more than once, a known issue for payment networks without central coordinating entities. Proof of work is the heart of the bitcoin network. If it did not exist, each member would be incentivized to modify the blockchain to benefit themselves. Lacking a centralized authority to resolve disputes, the network would cease to properly function.

Bitcoin's proof-of-work algorithm relies on the repeated running of hash functions. A hash function is a one-way mathematical operation that takes a string of data and transforms it into a fixed-length number called a hash. A hash is both deterministic and random: "Deterministic" because the result is always the same when identical data is passed through a hash function and "random" because the hash is unpredictable based on an input. It is important to note that each hash is unique to an input, making it like a digital fingerprint, and that the input cannot be calculated in reverse from the hash, which maintains privacy about the input.

Bitcoin relies on SHA-256 (Secure Hash Algorithm 256), which outputs a value that is 256 bits long. This output is usually displayed in base-16, meaning that digits range from 0-9 and then a-f. Despite looking like a mixture of numbers and letters, though, this output is purely a number. SHA-256 was created by the National Security Agency in 2001 as part of the SHA-2 family and is considered very secure.

Example:
Adding an "!" completely changes the hash.

Message: NYDIG
SHA-256 Hash: f08562886ddce54745bd29b1d
bf5e4b1ae54c34718938265a6b36b22917e8445

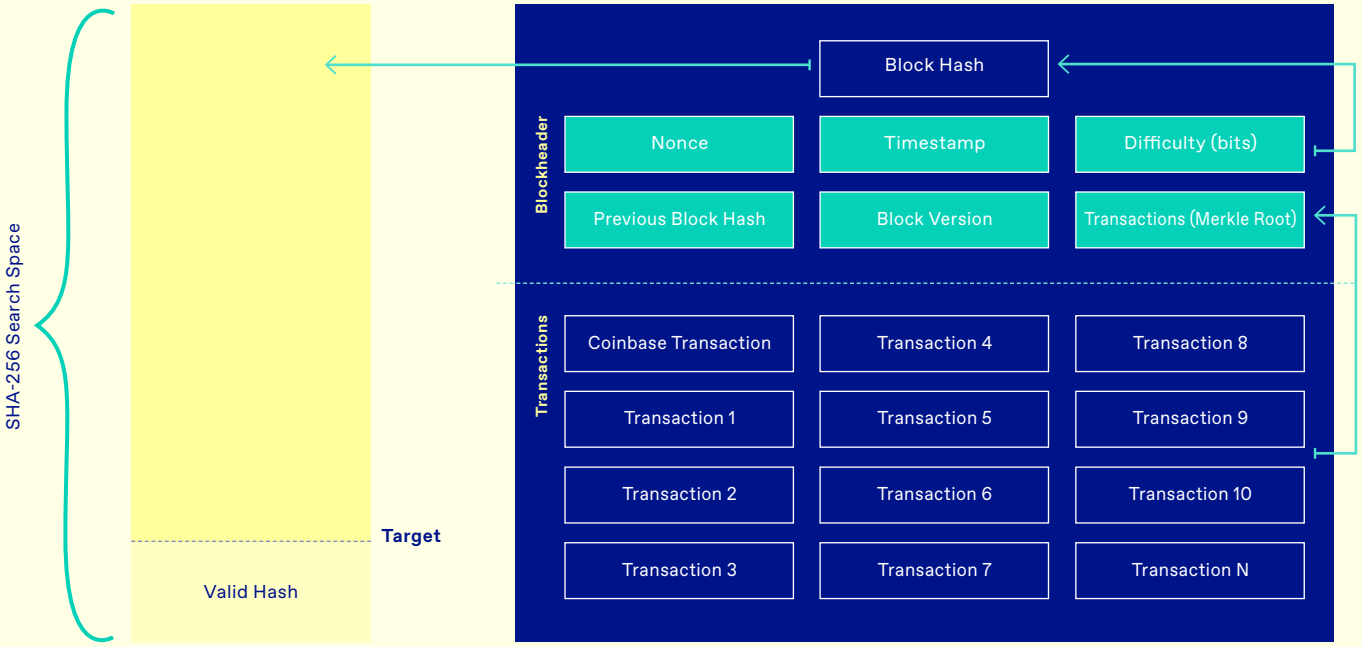
Message: NYDIG!
SHA-256 Hash: 45dc5108edee25df658f1300b0
a45c358243751e7bc3c1571aabb58fb4f36e80

Example:
Significantly adding text to a message does not change the length of the hash.

Message: It
SHA-256 Hash: 555c7b8b3856c5f4e5d6cd2 ec93
e4fc54678c49fd0d972d02608fab3ee7b37b3

Message: It was a bright cold day in April, and the clocks were striking thirteen.
SHA-256 Hash: 8ea71671a6edd987ad9e90974
28fc3f169decba3ac8f10da7b24e0ca16803bf0

To search for a valid proof of work, miners concatenate data from the block they are proposing, data from the previous block, a measure of the network's current difficulty level (to be explained more below), and an arbitrary number called a **nonce**, computer speak for "a number used only once." This string of characters is inserted into the SHA-256 hash function. If the output of the hash function is below a certain very low number called the **target,** a valid block is found, and the miner broadcasts it to the rest of the network. If not, the miner takes the same data, changes the nonce, and runs it again through the hash function. Because there's no way to predict the output of a hash function, miners are essentially engaged in trial and error. They take the required inputs and then change the nonce value until they come up with an output that is lower than the target. Presently, this takes on average 1.2×10^{23} guesses across all the miners in the bitcoin network for someone to find a valid proof of work. The rate at which the network is collectively trying new hashes is called the **hash rate** (SHA-256 hashes per second).



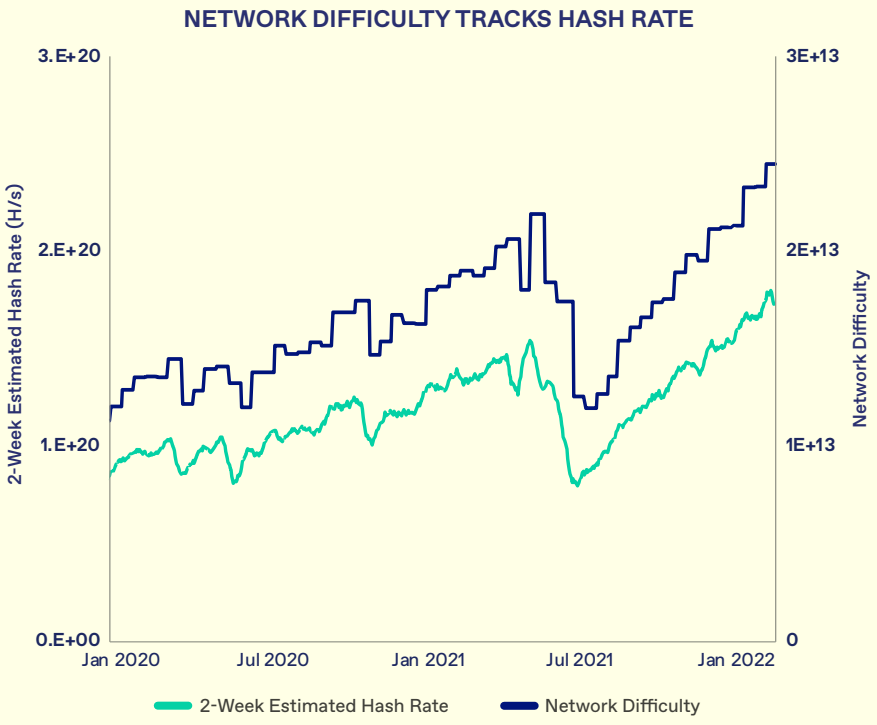
From this process, there are some important takeaways. First is that, because this is a highspeed random number guessing game, the probability a miner will find a valid block and create a proof of work is proportional to its share of the network hash rate. Size matters in Bitcoin mining and is one of the reasons mining entities join in so-called mining pools, which allow groups of miners to share the profits of whichever miner gets lucky. The second takeaway is that this is a competitive race for miners to find valid proofs of work. But once a valid proof of work is found by a miner, it is broadcast to the rest of the network to check, and if verified, becomes the block the rest of the miners build off and reference as an input for the next block. This chains proofs of work together, making it exceedingly difficult to reverse transactions in short order and impossible over time — an attacker would have to redo all the proof of work faster than the network creates new proof of work to reverse a previous transaction. This is the security function miners provide.

Miner Rewards

Miners receive two incentives to secure and propagate the blockchain — a **block subsidy** and **transaction fees** — collectively called the **block reward.** The block subsidy is an incentive issued to the miner of a block in the form of new bitcoins, currently set at 6.25 bitcoins per block. The block subsidy, whose programmatic design is described in more detail in the “Halvings” section, is also a way of increasing the circulation of bitcoins over time. Halving ensures the network’s fixed supply nature. Miners are also incentivized by transaction fees that are paid by the senders of bitcoins to induce miners to include their transactions in blocks. The block reward is the first transaction listed in any block, called a **coinbase transaction** — this is where the popular crypto exchange, Coinbase, gets its name. Unlike any other transaction, a coinbase transaction has no inputs, only outputs to the miner of the block.

Difficulty Adjustment

Bitcoin aims to produce a block every ten minutes on average. This interval was chosen to reduce chain splits (often referred to as forks), the appearance of two valid but competing blocks that can result because of the time it takes for newly broadcasted blocks to reach all miners. To continue to produce blocks at 10-minute intervals on average amidst changes in the network hash rate, Bitcoin changes the difficulty for miners to find valid proofs of work. It makes this adjustment every 2,016 blocks, about 2 weeks, in what is known as the **difficulty adjustment.** Difficulty is reduced to make it easier for miners to find blocks if they are taking longer than 10-minutes to be produced and raised to make it harder to find blocks if they have been coming faster than 10-minutes. Because the issuance of new bitcoins is directly tied to the creation of new blocks via the mining reward, this corrective measure also keeps the issuance of bitcoins at a steady rate and unaffected by mid-to-long-term changes in hash rate.



Source: btc.com, Glassnode

Halvings

It is well known that the number of bitcoins is capped at 21 million. This is enforced through block subsidy **halvings.** Every 210,000 blocks — roughly every four years — the Bitcoin network halves the block subsidy it pays to miners for creating new blocks. When the network launched in 2009, Bitcoin paid miners 50 bitcoins as a block subsidy. Today, three halvings later, Bitcoin issues 6.25 bitcoins per block and will do so until the next halving, estimated to occur in May 2024. Eventually, repeated halvings will programmatically reduce the block subsidy to zero in the year 2140. When the subsidy becomes zero, no new bitcoins will enter circulation. Bitcoin ensures this exhaustion because the smallest divisible unit of a bitcoin, called a satoshi (100 million satoshis are in each bitcoin) after Bitcoin's creator, is a 64-bit signed integer type that eventually can no longer be divided into whole numbers. Technically, the total number of bitcoins that will ever be created is 20,999,999.9769 at the final halving in the year 2140.

There are three important implications of this halving dynamic. First, all else being equal, the bitcoin revenue generated by miners through the block reward is decreased by 50% every four years. To keep dollar revenue to miners constant (assuming transaction fees stay the same), bitcoin's price in dollar terms must rise by 100%. Second, at halvings, the breakeven price to continue mining bitcoins doubles. This may push individual miners with outdated rigs to shut them off, allowing remaining miners to become more profitable. The third implication, and one that is long-term, is that because the block reward eventually goes to zero, miner revenue will come relatively more from transactions fees, which are paid by those on the network sending bitcoins.

Programmatic Supply Function

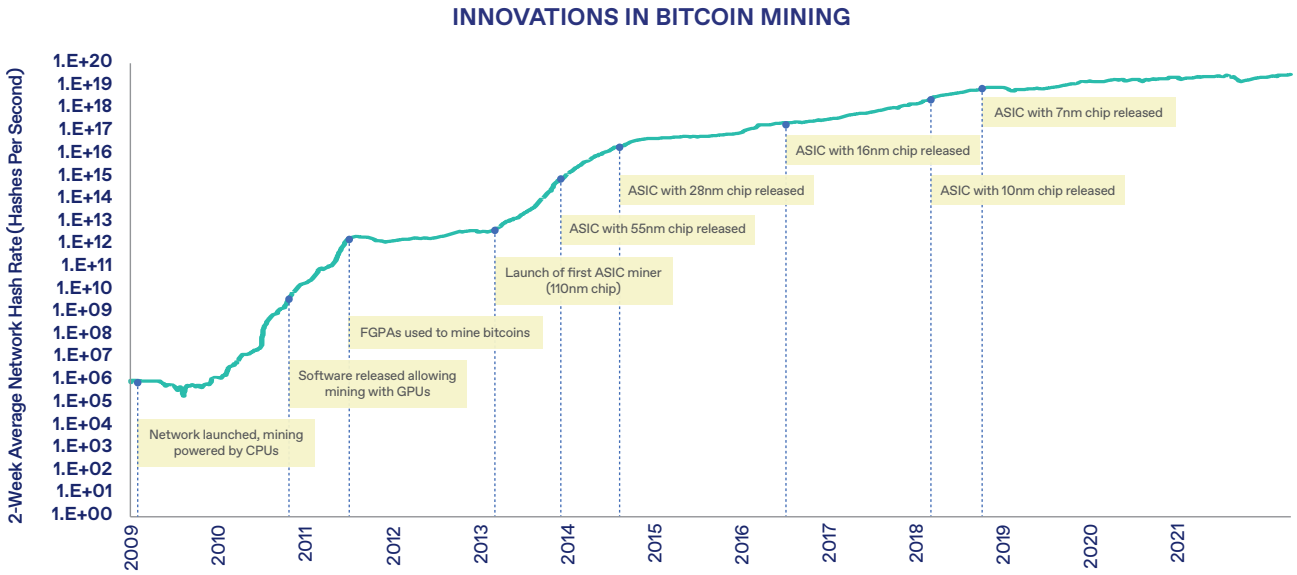
Bitcoin's difficulty adjustment and reward halvings are the bedrocks of Bitcoin's programmatic supply strategy. The difficulty adjustment ensures that the production of blocks, and therefore the supply of bitcoins, does not vary as network hash rate grows. In that respect, Bitcoin mining is unlike the mining of natural resources, where production can be affected by end market prices or improved extraction techniques. Changes in the hash rate that arise because of increased chip efficiency or machines being turned off and on only have an effect over the short term and are accounted for by the Bitcoin protocol every 2 weeks. In addition, reward halvings ensure that the production of bitcoins is steady over the intermediate-term but exhausts itself completely over the longterm. This assures that the supply of bitcoin is ultimately capped, a unique feature in both the natural and digital world. It is for this reason that bitcoin is often considered to be the world's "hardest asset." Even the gold supply has grown at 1% - 2% per annum since 1900, and there's no telling whether that growth rate might increase or decrease, unlike Bitcoin's programmatic supply.

PER BLOCK SUBSIDY (SATS)	ERA	HALVING	YEAR	BLOCK HEIGHT	NUMBER OF BITCOINS CREATED	STARTING BTC	ENDING BTC	PERCENT OF TOTAL
5,000,000,000	1	0	2009	0	10,500,000.000	-	10,500,000.0000	50.00000006%
2,500,000,000	2	1	2012	210000	5,250,000.000	10,500,000.0000	15,750,000.0000	75.00000008%
1,250,000,000	3	2	2016	420000	2,625,000.000	15,750,000.0000	18,375,000.0000	87.50000010%
625,000,000	4	3	2020	630000	1,312,500.000	18,375,000.0000	19,687,500.0000	93.75000010%
312,500,000	5	4	2024	840000	656,250.000	19,687,500.0000	20,343,750.0000	96.87500011%
156,250,000	6	5	2028	1050000	328,125.000	20,343,750.0000	20,671,875.0000	98.43750011%
78,125,000	7	6	2032	1260000	164,062.500	20,671,875.0000	20,835,937.5000	99.21875011%
39,062,500	8	7	2036	1470000	82,031.250	20,835,937.5000	20,917,968.7500	99.60937511%
19,531,250	9	8	2040	1680000	41,015.625	20,917,968.7500	20,958,984.3750	99.80468761%
9,765,625	10	9	2044	1890000	20,507.813	20,958,984.3750	20,979,492.1875	99.90234386%
4,882,812	11	10	2048	2100000	10,253.905	20,979,492.1875	20,989,746.0927	99.95117198%
2,441,406	12	11	2052	2310000	5,126.953	20,989,746.0927	20,994,873.0453	99.97558604%
1,220,703	13	12	2056	2520000	2,563.476	20,994,873.0453	20,997,436.5216	99.98779307%
610,351	14	13	2060	2730000	1,281.737	20,997,436.5216	20,998,718.2587	99.99389658%
305,175	15	14	2064	2940000	640.868	20,998,718.2587	20,999,359.1262	99.99694833%
152,587	16	15	2068	3150000	320.433	20,999,359.1262	20,999,679.5589	99.99847420%
76,293	17	16	2072	3360000	160.215	20,999,679.5589	20,999,839.7742	99.99923713%
38,146	18	17	2076	3570000	80.107	20,999,839.7742	20,999,919.8808	99.99961859%
19,073	19	18	2080	3780000	40.053	20,999,919.8808	20,999,959.9341	99.99980932%
9,536	20	19	2084	3990000	20.026	20,999,959.9341	20,999,979.9597	99.99990468%
4,768	21	20	2088	4200000	10.013	20,999,979.9597	20,999,989.9725	99.99995236%
2,384	22	21	2092	4410000	5.006	20,999,989.9725	20,999,994.9789	99.99997620%
1,192	23	22	2096	4620000	2.503	20,999,994.9789	20,999,997.4821	99.99998812%
596	24	23	2100	4830000	1.252	20,999,997.4821	20,999,998.7337	99.99999408%
298	25	24	2104	5040000	0.626	20,999,998.7337	20,999,999.3595	99.99999706%
149	26	25	2108	5250000	0.313	20,999,999.3595	20,999,999.6724	99.99999855%
74	27	26	2112	5460000	0.155	20,999,999.6724	20,999,999.8278	99.99999929%
37	28	27	2116	5670000	0.078	20,999,999.8278	20,999,999.9055	99.99999966%
18	29	28	2120	5880000	0.038	20,999,999.9055	20,999,999.9433	99.99999984%
9	30	29	2124	6090000	0.019	20,999,999.9433	20,999,999.9622	99.99999993%
4	31	30	2128	6300000	0.008	20,999,999.9622	20,999,999.9706	99.99999997%
2	32	31	2132	6510000	0.004	20,999,999.9706	20,999,999.9748	99.99999999%
1	33	32	2136	6720000	0.002	20,999,999.9748	20,999,999.9769	100.00000000%
-	34	33	2140	6930000	-	20,999,999.9769	20,999,999.9769	100.00000000%

History of the Bitcoin Mining Industry

When the Bitcoin network launched, there was little delineation between the hardware used for running nodes and miners. Many of the users who ran nodes on their computers were able to mine bitcoin profitably on those same computers. The “mining industry” as we know it did not exist. It developed gradually as the price of bitcoin — and thus the incentive to mine — grew.

The move toward industrialized mining was gradual. At the launch of the network, miners used standard at-home computers. These computers used the central processing unit (CPU) to mine. This period is commonly known as the CPU era. In October 2010, mining software was released that could use the graphics processing unit (GPU) of the computer. GPUs are better at running different computations in parallel than are CPUs and thus were more efficient at mining than CPUs. Miners squeezed every bit of efficiency out of GPUs by plugging together strings of the chips into a motherboard arranged to maximize heat dissipation. Cooling and energy usage quickly became limiting factors. Some miners could source cheap power production directly and used warehouse spaces to dissipate heat over larger spaces, foreshadowing the industrialized operations that are now commonplace. June 2011 brought further innovation; the use of field-gate programming arrays (FGPAs). FGPAs are integrated circuits that are programmable by end users. Miners found that these chips were much more energy efficient than GPUs and could be better scaled. But as bitcoin prices continued rocketing higher, a few enterprising individuals realized they could make massive gains in efficiency by programming algorithms directly into the hardware, and thus application-specific integrated circuits (ASICs) were born. This technology is the basis for all commercially viable mining rigs today. Progress has come through improvements in ASIC technology, especially as semiconductor foundries can produce increasingly dense chips.



Source: Glassnode

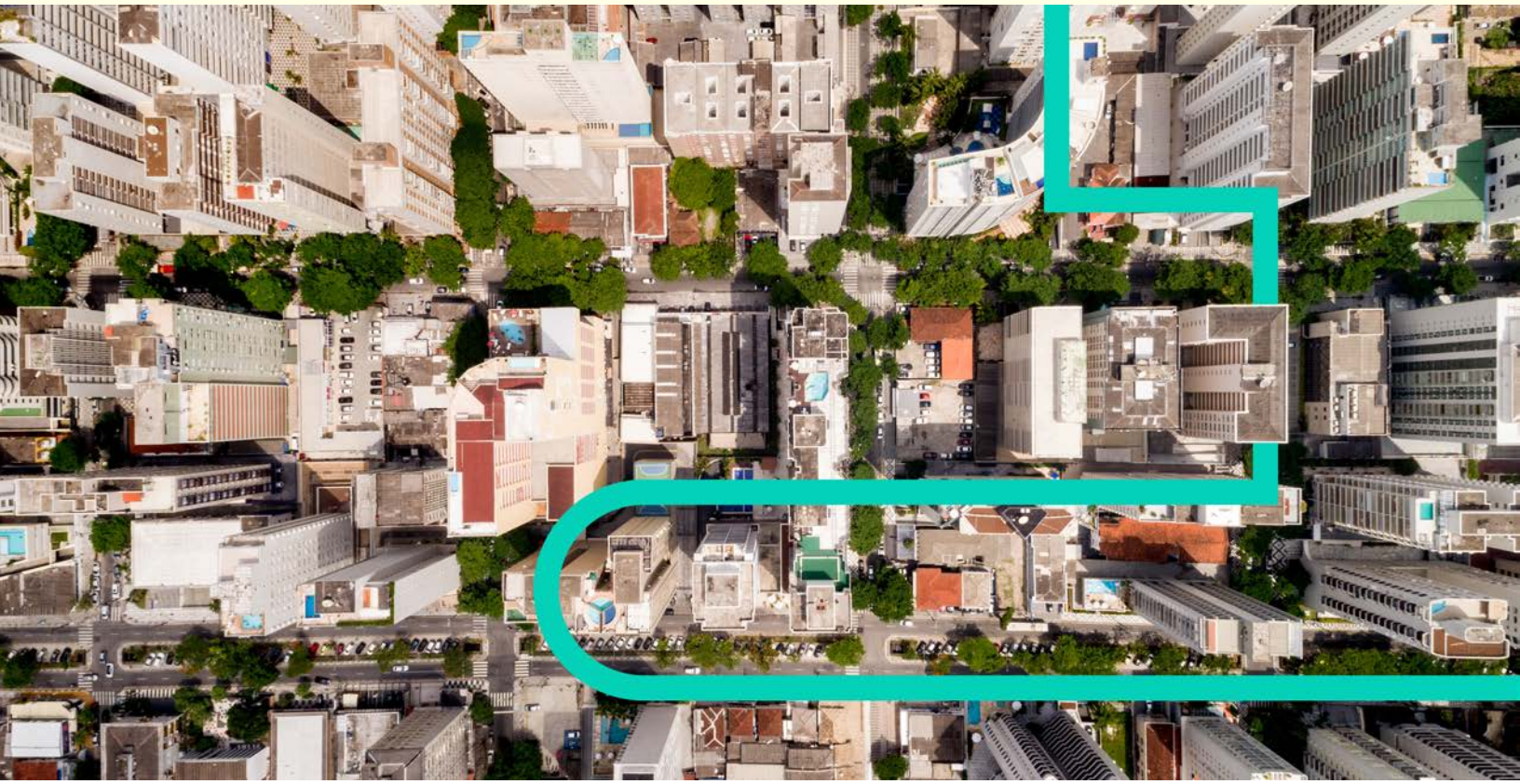
Mining rigs today look like gray metal shoeboxes with integrated fans, wires, and switches. They are heavy (for their size), loud (due to cooling fans), and use significant amounts of electricity. They are often deployed in racks at data centers. The rigs themselves are relatively mobile, a key distinction from natural resource extraction operations.

ASIC technology has rapidly improved from the first models. Efficiency gains came first from improved chips, but with chip improvements slowing, innovations have been made in different parts of the machine. The latest trend is immersion cooling (cooling rigs using dielectric fluids or water instead of air), which allows miners to run at higher rates for longer periods.

Although the machines are relatively simple to operate, complex supply chains, capital intensiveness, high electricity usage, and a high degree of competition mean that the mining industry requires contributions from several smaller subsectors, all of which work in tandem to secure the network (and generate profit).

BITMAIN'S S19 PRO 110 TH/S BITCOIN MINER

Source: Bitmain



Players in the Bitcoin **Mining Industry**

Like in other extraction industries, there are a variety of suppliers and service providers involved in the process of bitcoin mining. **ASIC miner manufacturers** are fabless semiconductor companies responsible for designing and assembling ASIC machines. They rely on upstream producers such as **semiconductor foundries** to create chips and **outsourced semiconductor assembly and test (OSAT)** companies to package and test those chips. Miners purchase machines either directly from manufacturers or through **ASIC miner brokers.** Miners then rely on **energy providers** to power the machines and **mining pools** to smooth their income. They also need a place to **host** the miners with enough space, strong internet, and sufficient power.

Semiconductor Foundries

Chip fabrication is a capital-intensive endeavor that requires significant research & development to stay ahead of the technology curve. At the onset of the industry, semiconductor firms often had their own foundries, but over time, the vast majority have chosen to design chips in-house and outsource their manufacturing to one of a few companies. There are currently only two foundries that can create competitive bitcoin mining chips, Taiwan Semiconductor Manufacturing Company (TSMC) and Samsung. Intel and SMIC were once in that group but both have fallen behind in the technological arms race. Intel's recent foray into the mining space has been as a manufacturer rather than as a foundry.

TSMC and Samsung's chip fabrication plants are huge operations that source much of the world's chips, so the lion's share of their activity is unrelated to crypto. As foundry customers, ASIC miner manufacturers typically do not enjoy top-tier status with their suppliers. That's because they buy less than, for example, Apple and their order volumes can be unpredictable because of ebbs and flows in crypto markets.

Outsourced Semiconductor Assembly and Test (OSAT)

After foundries create their chips, the chips need to be packaged and tested, a process known as OSAT. There is a small group of specialty companies that focus on this process. Like foundries, crypto is only a small part of what they do, though it is crucial step in creating mining rigs. Some of the companies commonly used by miners are STATS ChipPAC, Powertech Technology Inc. (PTI), and Advanced Semiconductor Engineering Inc. (ASE Group).

ASIC Miner Manufacturers

These companies design and source the underlying chips, assemble them into machines, and ship them across the globe. The industry is effectively a duopoly headed by Bitmain and MicroBT, though Bitmain is the larger of the two. Unlike in the two subindustries listed above, mining manufacturers are almost entirely crypto-focused. While they have attempted to diversify into other industries, especially artificial intelligence, the bulk of their revenue comes from selling ASIC miners, also known as mining rigs.

ASIC Miner Brokers

While large mining firms can directly source machines from manufacturers, much of the mining industry needs to work through brokers. Some of these brokers, like Luxor, are designed for large to medium-sized operations and contain minimum order sizes. Some, like Compass, cater to retail miners. These brokers will often package financing, hosting, and mining pool services to make it easier for the buyer to receive a holistic solution.

Miners

Mining companies buy ASIC miners and mine bitcoin. They source the machines either from manufacturers, from whom they can buy at a discount in bulk, or through brokers. They need to warehouse mining rigs, connect them to the internet, maintain them, and source energy. Energy is by far the most expensive variable operating expense, so a key to running an efficient operation is to obtain cheap energy. This topic will be discussed in more detail below, but this

is the reason many miners vertically integrate into energy production or focus on partnerships with existing energy companies. Mining can be viewed simply as a more profitable sink for energy than the grid as such and it has more recently garnered the attention of some of the world's largest power companies who have a significant amount of excess energy.

Industrial-scale crypto mining is still a relatively new industry so mining itself is not an extremely concentrated industry. The largest publicly traded miner today, Core Scientific, is responsible for about 4% of the network hash rate.

Mining Pools

Individual mining operations have a low hash rate compared to the network. A miner who purchases 1,000 units of the Antminer S19 Pro — the latest release from Bitmain that runs as much as $10,000 each — would only be expected to generate blocks on about 7% of days. Thus, a smaller operation has little hope of generating revenue with any regularity. Miners can smooth their income by joining a mining pool, which collects the efforts of constituent miners. Mining pools combine the efforts of their members to collect revenue more consistently, paying miners often daily based on their hash rates. Payment schemes to miners vary from pool to pool, but are largely based on the concept of a proportional share of revenue for the hash rate contributed to the pool.

There are few pure-play pool operators. Pool operators often have other businesses which range from manufacturing (Bitmain), operating an exchange (Binance), to providing software (Luxor).

	FULL PAY-PER-SHARE (FPPS)	PAY-PER-LAST-N-SHARES (PPLNS)	PAY-PER-SHARE +
Description	Miner receives expected block subsidies and transaction fees based on the overall share of the network.	Miner receives a portion of block subsidy and transaction fees actually mined the pool based on shares mined relative to other miners in the pool.	Miner receives expected block subsidy and share of actually mined transaction fees.
Pros	Miner receives steady income based on hash rate.	If the pool mines more bitcoin, then an individual miner can benefit.	Since received transaction fees are luck-based and subsidies are not, combines the pros and cons of FPPS and PLNS.
Cons	Mining pool collects any bitcoin mined beyond expectation.	Miner can receive unsteady income.	

Energy Providers

It is certainly possible for miners to simply plug their machines into the grid and draw power. However, they can often get better deals by striking agreements with grid operators or colocating to energy sources, which they may even operate themselves. Given that energy is by far the largest cost, the bulk of efficiency gains by miners are made in this sector.

Miners that collocate to energy plants are generally considered “behind the meter,” since they don’t need to purchase from the grid. Miners who are in front of the meter, especially the larger ones, often make deals with grids that allow them to purchase energy in bulk at a reduced rate. In exchange, miners who buy from the grid will often agree to turn off at times of high demand, what is known as curtailment. These deals highlight one of the big advantages of bitcoin mining; it is very easy to turn machines off and on, unlike for many other energy consumers.

Miners can also collocate to power sources and draw energy directly, either by building partnerships with the energy provider or even building the plants themselves. Similar to those that buy from the grid, in times of energy stress, collocated miners can turn off their machines and instead sell their energy back to the grid. There are several specialty operations in this field that tout their environmental bona fides, such as flared gas miners (which mine from potentially otherwise leaked methane emissions), solar, wind, nuclear, and even specialty miners like Stronghold Mining, uses energy from burning coal refuse.

Hosting Providers

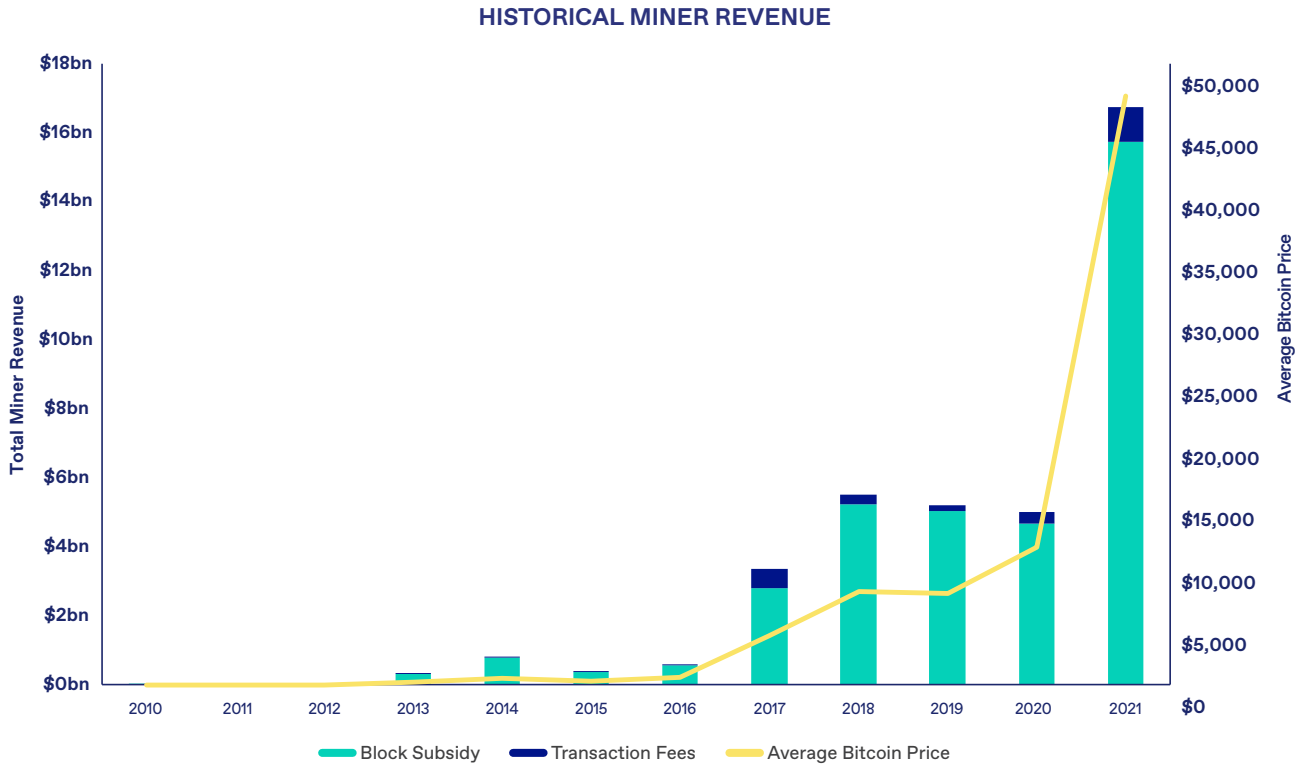
Big mining operations need rack space, heat exhaust, security, monitoring, and reliable electricity and internet access. Onsite technicians that can repair damaged equipment, update firmware, and manage overclocking settings — forcing the mining rig to go faster than it is intending to go — are also a big plus. Like in the rest of the mining industry, specialized players have emerged to provide these facilities and services. All hosts provide rack space and energy infrastructure; further services vary from host to host. Some more vertically integrated hosts might even own the energy source and directly deliver electricity.

Economics **Of Mining**

Miner Revenue

Miner revenue is driven by the block reward, which is composed of the block subsidy and transaction fees. The block subsidy, presently set at 6.25 bitcoins per block, is currently far and away the larger of the two sources of miner revenue. It has generally ranged from 90-100% of miner revenue since the start of the network. However, as we see further halving cycles, we may see this share decrease in favor of transaction fees. Transaction fees are paid by the senders of bitcoins as an incentive for miners to include their transactions in blocks. Since both revenue sources are denominated in bitcoin, the price of bitcoin weighs heavily on miners' earnings. The growth in miner revenue shown below is largely driven by bitcoin price.

Miner revenue is frequently contextualized as per-hash rate, meaning the amount of revenue that a miner can obtain for a unit of hash rate. This is called the **hash price.** To calculate this number, total daily miner revenue is divided by the total network hash rate.



Source: NYDIG, Glassnode

Miner Costs

The two largest miner costs are depreciation and energy costs. The former represents (on a delay) the degree of capital expenditure spent by a miner as their equipment slowly becomes useless. For vertically integrated miners, it may also capture depreciation of power plant equipment, so their depreciation costs can be a lot higher. While hefty, depreciation costs are not marginal, meaning that they do not factor into the breakeven price of bitcoin. Buying a rig is a sunk cost; once you have it, the decision to turn it on depends on the cost of running it versus the revenue. The largest marginal cost of bitcoin mining is, by far, that of electricity. As of the current writing of this report, breakeven prices are well below bitcoin prices. As more miners come online and the difficulty increases, that spread will likely shrink. And as breakeven prices approach the actual price of bitcoin, the difference between successful and unsuccessful miners will likely be the ability to obtain reliable electricity and mining equipment at low prices. Other costs that miners face include hosting costs, machine maintenance, mining pool fees, and SG&A.

Mining **Misconceptions**

IF MORE MINERS JOIN THE NETWORK, MORE BITCOINS WILL BE MINED

The Bitcoin network is designed so that one block is created every ten minutes, on average. This is handled through difficulty adjustments. If more miners join the network, in a vacuum that should increase the rate blocks are mined. Every two weeks, however, the network adjusts. The protocol checks how many blocks were mined in the preceding two-week interval and then adjusts the difficulty for mining a block so that, based on the data it gathered, the block mining rate should average one per ten minutes. That said, because of the two-week lag in the difficulty adjustment and the growth rate of the hash network, the long-term rate has been a little bit faster than one-per-ten minutes (closer to one-per-9.5 minutes).

HASH RATE DETERMINES BITCOIN PRICE

Because the same number of bitcoins are created every ten minutes during any given halving epoch, bitcoin's supply is perfectly inelastic — that is, supply does not increase or decrease in response to price. No other industry operates under this condition. Instead of price, the lever that is adjusted is the network difficulty. When it becomes harder to mine a bitcoin, though, this increases the marginal cost of production. So marginal cost and price should theoretically converge, but rather than price converging on marginal cost, marginal cost converges onto price. This means that mining activity should theoretically not have any impact on price. Rather, price influences the level of mining activity. This was explored in a 2020 academic paper by Fantazzini and Kolodin titled "Does Hashrate Affect the Bitcoin Price?"

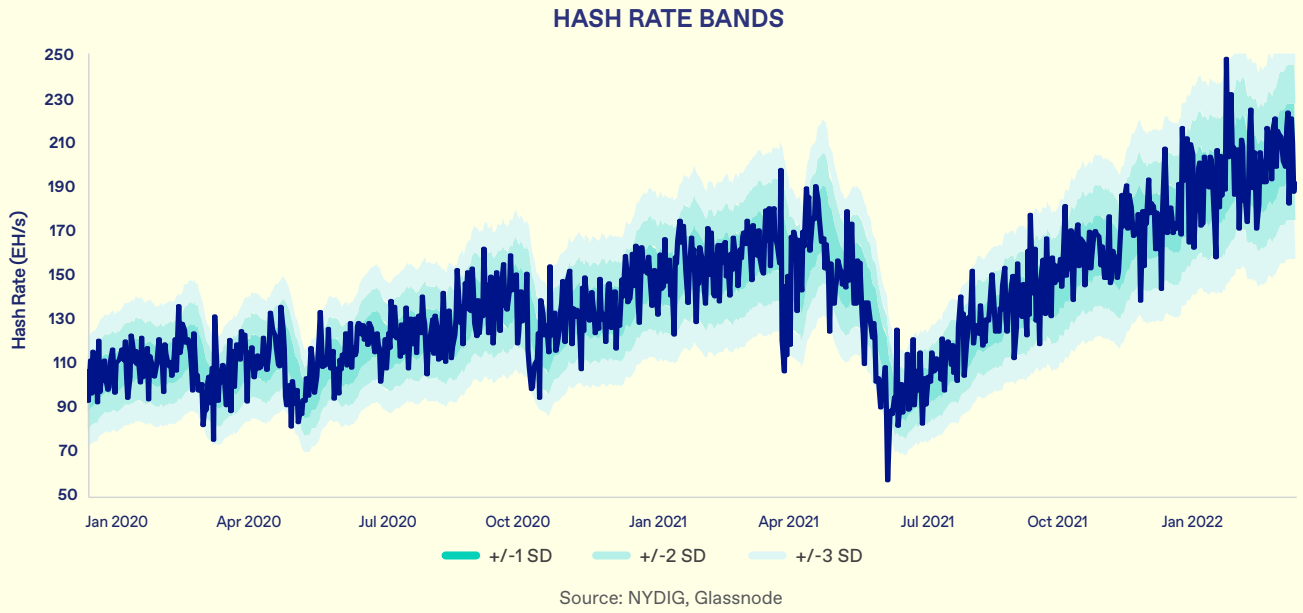
INCREASES IN HASH RATE ARE CAUSED BY INCREASES IN ELECTRICITY CONSUMPTION

Mining rigs have made extreme gains — more than 300x, though this pace has slowed down — in energy efficiency since the first ASIC was launched in 2013. When the hash rate of the network increases, it is often because more mining rigs are plugged into the grid, but it can also result from the increased efficiency of subsequent generations of miners. This logic cuts both ways. Bitcoin mining is an operation that converts electricity into bitcoins. As long as bitcoin's price is above a miner's breakeven, the goal of a miner is to convert as much electricity as possible into bitcoins. When more energy-efficient machines are produced, this does not mean that miners consume less electricity, it means that they get more bitcoins out of their electricity.

NETWORK HASH RATE CAN BE DIRECTLY MEASURED

The Bitcoin network is a decentralized distributed network. Unlike a data center, where each machine's status is directly monitored by a centralized operator, miners in the Bitcoin network only emit completed blocks. As such, the only way to measure the hash rate is to observe the difficulty in creating a block and the number of blocks produced in a certain period, generally over 24 hours.

But there's a further complication: even if the true hash rate remains unchanged, there can be variations in the number of blocks produced due to random noise. That's because bitcoin mining is probabilistic. The number of blocks produced in any given period can be above or below expectations. The number of blocks produced follows an approximately normal distribution (technically a Poisson distribution) centered around 144 blocks (based on one block every ten minutes) with a standard deviation of 12 blocks. So daily network hash rate measures are estimates that can contain significant statistical noise.



Source: NYDIG, Glassnode

MINED COINS CAN BE SOLD OR MOVED IMMEDIATELY

Newly minted coins, those created by the block subsidy, are not immediately spendable. Bitcoin has a maturation period for newly created coins of 100 blocks, 16 2/3 hours on average, after which newly mined coins can be moved. This is designed to protect against the double-spending of the block subsidy. If two blocks are simultaneously mined, this can result in a fork, in which two valid and competing chains are propagated around the network. When a new block is built off one of the competing chains, it is recognized as the canonical and longest chain with the greatest amount of accumulated proof of work. The shorter and thus losing chain is no longer recognized, a term called "orphaned." Any block subsidy associated with the shorter chain is not recognized by the miner and any transactions in the block are returned to the mempool. The 100-block maturation time is intended to prevent the spending of the block subsidy from the soon-to-be orphaned blockchain.

BLOCKS ARE SEQUENTIALLY TIME-ORDERED

While timestamps of blocks are recorded in the blockchain, these measures can be notoriously unreliable. This is due to the way that blocks are currently mined. In the early days of the network, to find a valid block hash, miners would simply need to try out a variety of nonces. However, as the difficulty has drastically increased from the early days of the network, just varying the nonce is often an insufficient source of entropy to generate a valid block hash. This means that miners need to alter other variables. One of these variables is the block's timestamp. A timestamp is considered valid if it is greater than the median timestamp of the previous 11 blocks and less than two hours after the median of the current network time returned by all nodes connected to the miner. So timestamps are generally accurate only within an hour or two. As a result, block timestamps are unreliable and are often not in chronological order. It is common to see older blocks, those with lower block heights, have more recent timestamps than newer blocks. The correct ordering of transactions, therefore, is by block number (block height). It is also the reason Satoshi Nakamoto, pseudonymous creator of Bitcoin, initially referred to the blockchain as a "time chain."

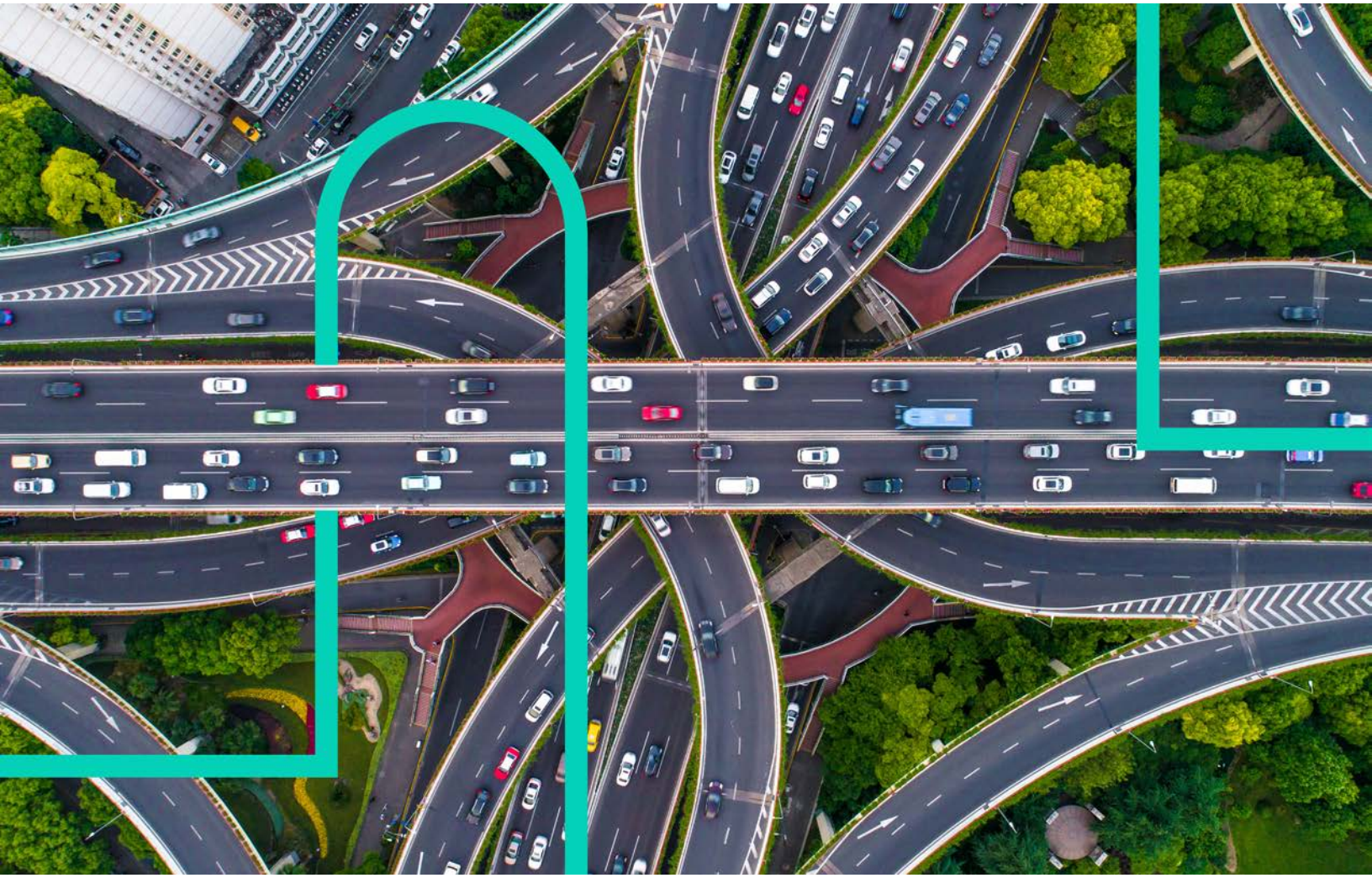
CHANGES IN NETWORK HASH RATE IMMEDIATELY CHANGE MINER PROFITABILITY

It is often thought that when the network undergoes a sudden change in its hash rate, miner profitability falls or rises. This is only true after the next difficulty adjustment. Sudden changes in network hash rate on their own do not immediately make it harder or easier for remaining miners to find blocks. We will use a fictitious example to demonstrate. Let's say that on the first block of a difficulty period, the 2,016 block adjustment window that Bitcoin uses to calculate the next difficulty, half of the mining network suddenly goes offline. Because the difficulty of finding new blocks remains the same, and only half the network hash rate remains, it will take remaining miners twice as long to find valid blocks. Block times double from 10 minutes to 20 minutes and, instead of producing 144 blocks per days, miners only produce half that, 72 blocks per day. The 2,016 difficulty adjustment window instead of taking 2 weeks, will take a month. During this period, miners, as an aggregate, make half as much per day on the block subsidy as they normally would. But remaining miners have a higher proportion of the network hash rate, so each miner's daily revenue stays the same (in expectation) during this period. When the difficulty adjusts, however, blocks will return to being produced 144 times a day and thus remaining miners will then each make twice as much on a daily basis. This analysis omits any potential changes associated with transaction fees, which would likely go up during the original difficulty period as competition for scarce block space goes up.

	ORIGINAL	50% HASH RATE REDUCTION	AFTER DIFFICULTY ADJUSTMENT
Description	100	50	50
Number of Blocks per Day	144	72	144
Block Subsidy per Block (BTCs)	6.25	6.25	6.25
Dailly Block Subsidy (BTCs)	900	450	900
Miner Hash Rate (EH/s)	10	10	10
Miner Hash Share	10%	20%	20%
Daily Miner Revenue (BTCs)	90	90	180

MINERS CONTROL BITCOIN

For many years, there was a commonly held belief that miners controlled Bitcoin. After all, miners decide which transactions should or should not be included in a block, so they can exclude transactions that follow a different protocol to their preference. This belief, however, was severely weakened during a tumultuous time in Bitcoin's history known as the block size debate. From 2013 until 2017, the Bitcoin community, including miners, exchanges, developers, investors, and other constituents were engaged in a heated debate on whether the transaction throughput of Bitcoin should be scaled. Miners, who were generally in favor of increasing the throughput, believed they could use their influence to force the issue, but they were unsuccessful. Ultimately, this led to an irreconcilable fissure in the community that resulted in the creation of Bitcoin Cash, which forked from Bitcoin on August 1, 2017. The lesson from this rancorous period was that Bitcoin is controlled by its user base rather than any one constituent. While at its core Bitcoin is a software program, the broader construct of Bitcoin is largely a social phenomenon, one defined by the common agreement on what constitutes Bitcoin. At the end of the day, the Bitcoin community decided what Bitcoin was, with the minority of dissenters coalescing around other digital assets like Bitcoin Cash.



Glossary

NAME	DEFINITION
Address	A public-facing alphanumeric string that can own bitcoin balances on the blockchain.
ASIC miner brokers	Organizations that facilitate the buying and selling of ASIC miners.
ASIC miner manufacturers	Fabless semiconductor companies responsible for designing and assembling ASIC machines.
Blockchain	A shared database that accounts for user balances of bitcoins.
Block reward	The miner's reward for mining a block, equal to the sum of the block subsidy and transaction fees.
Block subsidy	An incentive issued to the miner of a block in the form of new bitcoins, currently set at 6.25 bitcoins per block.
Coinbase transaction	The first transaction listed in a block, directed towards the miner, which includes the block reward.
Curtailment	Turning off ASIC miners at time of high energy demand in order to reduced stress on the grid.
Difficulty	A measure that is reset every two weeks based on realized hash rate to ensure that blocks appear once every ten minutes on average.
Difficulty adjustment	Adjustments to the difficulty of mining blocks, made every two weeks so that the average rate of solving new blocks is, on average, on-per-ten-minutes.
Digital signatures	A cryptographic technology allowing a user to prove ownership of bitcoins on the blockchain.
Energy providers	Providers of energy to run ASIC miners.
Forks	A fork occurs when two separate versions of the blockchain emerge, either because of simultaneously solved blocks or changes in the underlying code.
Halvings	50% reductions in the block subsidy made once every 210,00 blocks (roughly every four years).
Hash	The process in which miners attempt to create valid blocks by varying a nonce and hashing the block header.
Hash algorithm	A cryptographic algorithm that generates deterministic, fixed-length, and seemingly random "fingerprints" for a set of data.
Hash-based proof of work	The process by which miners collectively hash block data to make the blockchain immutable.
Hash price	The amount of revenue that a miner can obtain for a unit of hash rate.
Hash rate	The rate at which miners can try new hashes to create valid blocks.
Mempool	The pool of data (memory pool) in which prospective transactions sit before being included into new blocks.
Miners	Companies (or individuals) that own mining rigs and run them to collect the block reward.
Mining pools	Groups of miners that collect and redistribute block rewards to better smooth income for individual miners.

Nonce	An arbitrary number varied by miners in order to create a valid block.
Outsourced semiconductor assembly and test (OSAT)	Assemblers, testers, and packagers of testers of ASICs (amongst many other kinds of chips).
Semiconductor foundries	Pure-play chip fabricators used to produce ASIC chips (amongst many other kinds of chips).
Software providers	Creators of software that help run ASIC miners.
Target	A very small number. To mine a valid block, miners must hash a number smaller than the target.
Transaction fees	Fees paid by the senders of bitcoins to induce miners to include their transactions in blocks.

DISCLOSURES

This report has been prepared solely for informational purposes and does not represent investment advice or provide an opinion regarding the fairness of any transaction to any and all parties nor does it constitute an offer, solicitation or a recommendation to buy or sell any particular security or instrument or to adopt any investment strategy. Charts and graphs provided herein are for illustrative purposes only. This report does not represent valuation judgments with respect to any financial instrument, issuer, security or sector that may be described or referenced herein and does not represent a formal or official view of New York Digital Investment Group or its affiliates (collectively, "NYDIG").

It should not be assumed that NYDIG will make investment recommendations in the future that are consistent with the views expressed herein, or use any or all of the techniques or methods of analysis described herein in managing client accounts. NYDIG may have positions (long or short) or engage in securities transactions that are not consistent with the information and views expressed in this report.

The information provided herein is valid only for the purpose stated herein and as of the date hereof (or such other date as may be indicated herein) and no undertaking has been made to update the information, which may be superseded by subsequent market events or for other reasons. The information in this report may contain projections or other forwardlooking statements regarding future events, targets, forecasts or expectations regarding the strategies, techniques or investment philosophies described herein. NYDIG neither assumes any duty to nor undertakes to update any forwardlooking statements. There is no assurance that any forward-looking events or targets will be achieved, and actual outcomes may be significantly different from those shown herein. The information in this report, including statements concerning financial market trends, is based on current market conditions, which will fluctuate and may be superseded by subsequent market events or for other reasons.

Information furnished by others, upon which all or portions of this report are based, are from sources believed to be reliable. However, NYDIG makes no representation as to the accuracy, adequacy or completeness of such information and has accepted the information without further verification. No warranty is given as to the accuracy, adequacy or completeness of such information. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions that occur subsequent to the date hereof.

Nothing contained herein constitutes investment, legal, tax or other advice nor is it to be relied on in making an investment or other decision. Legal advice can only be provided by legal counsel. NYDIG shall have no liability to any third party in respect of this report or any actions taken or decisions made as a consequence of the information set forth herein. By accepting this report, the recipient acknowledges its understanding and acceptance of the foregoing terms.