

Twelfth CryptoSuper 500 Report

Bitcoin Passes the Fourth Halving

Stephen Perrenod

May 2024

Note: This research report is an analysis of the technologies and trends surrounding proof of work cryptocurrencies. It is not, and must not be considered as, financial, investment, or legal advice. Disclosure: As of this date, author has long positions in MicroStrategy and Bitcoin ETFs but no positions in Bitcoin mining stocks.

“Bitcoin is a specialized AI that is incentivizing and organizing human networks of value, in a symbiotic manner, adhering to power laws, based on a Zettascale supercomputer network” - @moneyordeb

Bitcoin is a Decentralized Special Purpose Supercomputer

Bitcoin is the world's largest special purpose supercomputer. And it is globally decentralized. Millions of nodes all run the same open-source code to secure the Bitcoin network, create value, and put new transactions onto the distributed ledger.

The latest Top500 list has just been announced at the ISC 2024 conference in Hamburg, and once again the Frontier supercomputer with 1.2 Exaflops peak performance is number one on the list. If assigned to SHA-256 hashing, Frontier would provide only the equivalent hash rate of about three cabinets of the latest high-end Bitcoin mining systems, costing less than 0.1% of Frontier's cost.

Michael Saylor, Chairman of MicroStrategy, has pointed out that GPUs are two orders of magnitude slower than the 5-nanometer technology of custom ASICs used for Bitcoin mining today. He makes the point that the Bitcoin network is unassailable by all of the hyperscale computing resources combined in AWS, Google, and Microsoft Azure cloud data centers today.

Bitcoin Grows as a Power Law

Bitcoin is now a trillion-dollar asset, and its annual mining revenue is above \$10 billion. Most of the supply of this finite asset, 19.7 million out of the ultimate 21 million, has already been produced. Some call it digital gold, but the new supply rate as of the Fourth Halving cut in supply emission on April 20, 2024 (UT), has dropped below 0.8% per year. This is half of the rate of gold's annual supply increase.

The lack of new supply and the high level of security from millions of Bitcoin mining computer systems (“rigs”) in what is effectively a globally decentralized supercomputer of cooperative competition has attracted a rapid growth in the Bitcoin network over its history. Roughly speaking, the total address count of wallets has grown as the cube of the age of Bitcoin. If one applies Metcalfe's law, which says that the value of a network should grow as the square of its size, and then one would expect Bitcoin to have grown in value by roughly the sixth power. This is steeper than a parabolic or cubic relation, it is basically the product of a parabola with a cubic relation. The theory around this has been developed by PlanG, originally in 2012. This report's writer also independently realized and published about the Power Law nature of Bitcoin 5 years ago. Here is a brief YouTube video on the power law behavior:

OrionX Constellation™ reports cover six Es: big trends (Envision), industry milestones (Events), historical view of a technology segment (Evolution), main vendors in a market segment (Environment), customer decision criteria (Evaluation), and how vendors in a segment score (Excellence) based on the OrionX methodology, which considers market presence and trends, customer needs and readiness, and product capabilities and roadmap.

©2023 OrionX.net

<https://www.youtube.com/watch?v=DYfLbCZJWqY>

YouTube video: *Quantonomy, the Bitcoin Power Law Theory (10 minutes)*

And a power law is indeed the case. The chart below is a log-log chart (using log base 10), of Bitcoin's market cap value, and the relationship is a straight line, indicating a power law is in effect. The slope of the power law is 6.4. That is, as Bitcoin grew from age 1 ($\log_{10} = 0$) to age 10 ($\log_{10} = 1$), one order of magnitude, its market cap grew by over 6 orders of magnitude, a factor of more than a million.

Since age of just one year at only \$10,000 market cap, it grew to tens of billions of dollars at age 10 and now at age 16 block years it has a market cap of over \$1 trillion. One block year is 52,500 blocks on the Bitcoin timechain and is close to a calendar year. That is over eight orders of magnitude, a factor of a hundred million, during just 1.2 factors of ten of elapsed time in years.

The best fit regression shown in the chart below is 6.4 in the power law of index with a very high R^2 of 0.97. In recent years market cap has grown more similarly to the price power law since most of the supply has been created already; the price growth is also a power law of high statistical confidence, at around the 5.4 (5.7) power of Bitcoin's age in block years (calendar years).

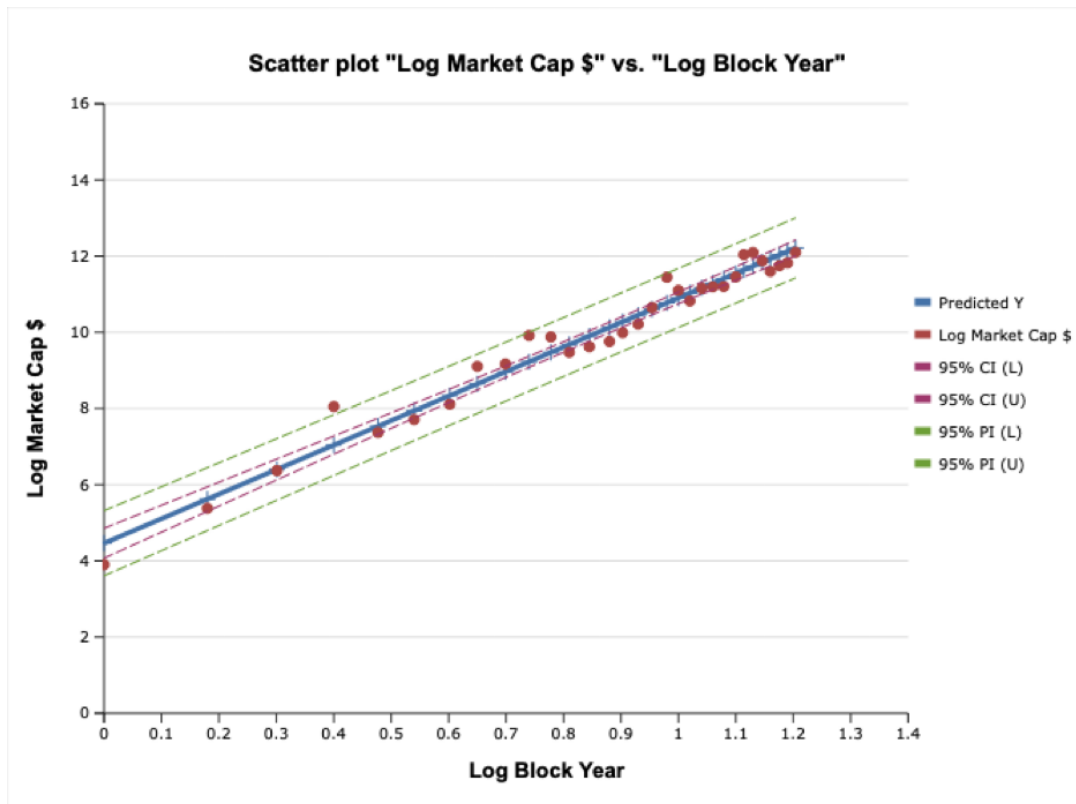


Figure 1. A \log_{10} - \log_{10} chart of Bitcoin's market cap vs. block year, age of the Bitcoin block chain. The straight line indicates a power law, and the slope of the line indicates a steep power law of over the 6th power. Volatility is high, over a factor of two in linear terms, and yet the R^2 is a very high 0.97. The green dashed line shows the plus or minus two standard deviation contours, i.e. the volatility is shown at two sigma confidence levels.

Bitcoin “Flippens” Meta and Berkshire Hathaway

There used to be hope in the Ethereum community that its market cap would eventually ‘flippen’ or pass above Bitcoin’s market cap. This was never in the cards, and even more so after Ethereum abandoned proof of work in September 2022. Since then, its value has fallen when measured against Bitcoin.

The real ‘flipping’ has been the rise of Bitcoin’s market cap above that of all but six publicly traded stocks. Only the five most valuable stocks (“MANGA”) plus Saudi Aramco are worth more in market capitalization than the Bitcoin network. Since our prior 11th report filed in November of last year, Bitcoin has passed both Berkshire Hathaway and Meta (Facebook) in market cap, as that increased from \$725 billion to \$1.25 trillion, around a 72% increase in half a year.

Proof of Stake, Proof of Authority, Proof of Work

Trust, Consensus	Who	What (currency)	Where
Proof of Stake	Crypto founders, companies	ICO token (equity)	Centralized ledger or partially decentralized blockchains
Proof of Authority	Governments	US \$, Euro, other fiat	Centralized ledgers (Fed, banks)
Proof of Work	Miners	Bitcoin, other PoW coins	Public decentralized blockchain (full nodes)

Table 1. Major classes for consensus of financial ledgers. Proof of Stake in the crypto world is analogous to shares in a consortium or cooperative or decentralized corporation, those who hold more stakes have more consensus votes and more dividends from staking. Governments hold a monopoly on the issuance of fiat under their legal authority. Proof of Work coins, most notably Bitcoin, are privately generated and rely on electricity and cryptographic hashing for creation of the currency.

Cryptocurrencies use consensus algorithms to validate transactions onto a blockchain, and to avoid double spending or counterfeiting. They are digital assets only and are held in a partially or highly decentralized ledger, typically in a blockchain form. In a blockchain, each block is linked to the prior block via a cryptographic hashing technique.

Fiat currency is issued by a central governmental authority and uses a variety of techniques to secure the digital representations and physical instances, to limit counterfeiting of the currency.

Proof of Stake cryptos, such as Ethereum since September 2022, use some type of voting scheme, including election of validators, to determine which transactions are approved and enter the ledger. Voting power depends on staking tokens, those who own more get more votes. Little compute power is employed in this effort.

Proof of Work (POW) on the other hand requires supercomputing levels of computational and electrical power for validating blocks onto the blockchain. Proof of work uses a cryptographic hash lottery in which the effective number of chances to win depends on the computational power devoted to a cryptographic hash puzzle. The resultant power is measured in hashes per second for the algorithm in question.

Methodology and Top POW Coins

This is a cryptocurrency supercomputer report, so we restrict our analysis to those cryptocurrencies that use significant amounts of computer power for their creation, or minting. And that means Proof of Work. That means substantial computational power required to create the asset in question. And POW underpins security substantially as well as value. Table 2 shows the six coins with over \$1 billion market cap.

The highest hash rate by far is Bitcoin’s 600 Exahashes/second (600 billion billion). The number two mined coin by annual value is Dogecoin with 1 Petahash/s, which is a factor of 600,000 lower. Now the two use different

algorithms, SHA-256 hashing for Bitcoin and a less compute intensive Scrypt in the case of Dogecoin so the two hashrates are not directly comparable. But the relative value of the two networks is. And Bitcoin is 60 times as valuable as Dogecoin.

While Bitcoin requires millions of systems to provide the total global hash rate, Dogecoin is only in the hundreds of thousands; just 60,000 of the latest Scrypt high end systems could provide all the global Scrypt hash rate for Doge.

The most significant of the hard forks of Bitcoin, created in 2017, is Bitcoin Cash and it has less than 1% of original Bitcoin's hashrate and less than 1% of its value, despite employing the identical SHA-256 hashing algorithm.

Coin	Market Cap (B\$)	Total hash rate and Algorithm	Annual Production rate \$B (nominal)	Current Supply (millions)	Max Supply (millions)
Bitcoin	1288	575 Exa, SHA-256	10.73	19.69	21
Dogecoin	24	1.05 Peta, Scrypt	0.88	144,200	infinite
Litecoin	10	1.12 Peta, Scrypt	0.12	74.5	84
Bitcoin Cash	6	3.67 Exa, SHA-256	0.08	19.7	21
Ethereum Classic	4	159 Tera, Random X	0.17	146.9	210.7
Monero	2	2.52 Giga, ETCHash	0.02	18.4	infinite

Table 2. Top POW coins by market cap. Also provided are the total hash rate (as of 5/15/24) and the algorithm used for hashing, the current value of the annual rate of production (not including fees) and supply, both total minted to date and ultimate maximum possible.

Hashing Algorithms, Technology

SHA-256 is a member of the SHA-2 family of hashing algorithms, developed and patented by the NSA and publicly released in a royalty free manner via NIST in 2002.

SHA-256 uses a “nonce” random guess and performs a double hashing algorithm including the hash of the prior block for chaining purposes, and with the desire that the hashed result, an unsigned integer, is smaller than some target. And that target size is inverse to the growing difficulty, where the difficulty is a Nakamoto consensus parameter regularly adjusted to keep block times close to 10 minutes.

If block times kept getting shorter and shorter with more and faster hardware engaged with the Bitcoin network then synchronization of the ledger, stored in thousands of full nodes around the world, would have failed years ago and decentralization would have been lost.

Additionally keeping the block time close to uniform enforces Bitcoin's monetary policy of approximately regular issuance over time but with halving of the block subsidy reward repeatedly each four years.

The need for the regular difficulty adjustment, in the face of Moore's law and of growing Bitcoin adoption, was a critical insight.

Bitcoin minting started with CPUs then switched to GPUs within a couple of years, those provided about an order of magnitude performance increase. By 2013 the switch to much faster ASICs was underway; these provide speed ups of an additional two orders of magnitude. These ASICs are pipelined and have multiple functional units and /or cores but the details are proprietary. The latest versions from the two principal vendors in the space, Bitmain and MicroBT, use 5 nanometer silicon devices fabbed at TSMC and Samsung, respectively.

Both vendors are Chinese companies yet using fabs in Taiwan and Korea. Given that Bitcoin is now being examined for security applications (MicroStrategy for one, just announced an identity solution for enterprises) one wonders if Bitcoin hash rate generation could become a national security issue. Jason Lowery's MIT thesis, **Softwar**, is entirely about that possibility for Bitcoin.

Block, owned by Jack Dorsey, has completed development on their 3 nm Bitcoin mining chip and is working on a full bitcoin mining system.

Because there are now millions of mining rigs even hyperscalars like Amazon and Microsoft are unable to mount a 51% attack on the Bitcoin network, it would require deploying several billion CPUs or hundreds of millions of GPUs. Apparently, only Bitcoin miners are buying the specialized ASIC rigs, but that is beginning to include small nation-states.

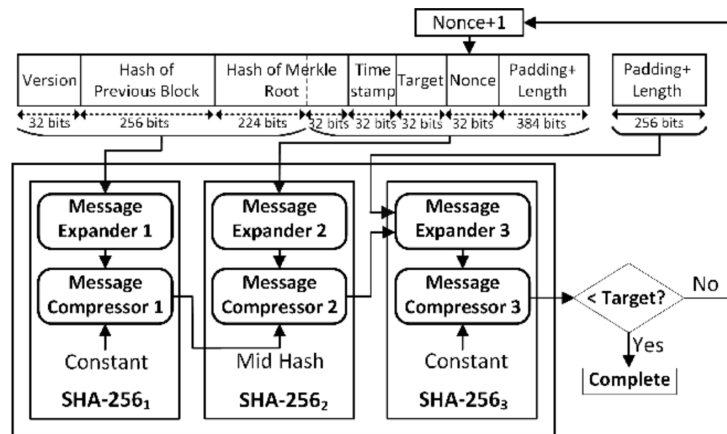


Figure 2. Diagram of SHA-256 hashing algorithm. From H. L. Pham, T. H. Tran, T. D. Phan, V. T. Duong Le, D. K. Lam and Y. Nakashima, "Double SHA-256 Hardware Architecture with Compact Message Expander for Bitcoin Mining," in IEEE Access, vol. 8, pp. 139634-139646, 2020, doi: 10.1109/ACCESS.2020.3012581.

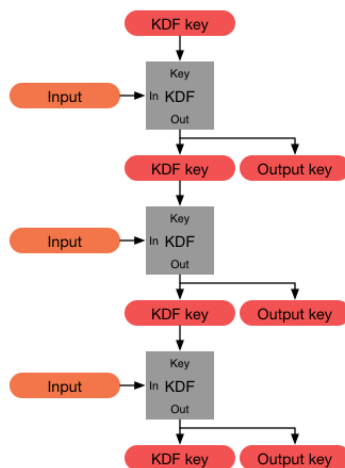


Figure 3. Key distribution function, used to build a chain. This is the computational kernel of the Script hashing algorithm. Computational work is required to generate the key.

New and Recent Mining Rigs

Millions of mining rigs are deployed around the world in the Bitcoin minting and fee collection business. Individually they produce between 100 Terahashes/sec and 400 Terahashes/sec, and collectively they produce 600 Exahashes/sec. Table 3 shows the newest and most competitive and energy-efficient systems.

Two vendors dominate the list, both are Chinese companies, but the ASICs are sourced in Taiwan and South Korea. The single fastest mining rig available for shipment as of May 2024 is the Whatsminer 36S water-cooled system from MicroBT, generating 390 Terahashes, and consuming over 7 kiloWatts of power; it has a retail price of \$13,700.

Post-halving, even with reduced block subsidy, these mining rigs are profitable on an operating basis with 5 cent per kWh electricity. But that does not include the capitalization of their cost.

So that you understand the scale of the mining challenge, a system with 390 Terahashes/sec has 2/3 of a millionth of the global hash rate and might earn of order \$0.50 per hour after electricity cost by directing its hash rate to a shared rewards pool.





















 MicroBT WhatsMiner M63S	Nov 2023	390 Th/s	7215 W	50 db	SHA-256	\$12.18 /day
 Bitmain Antminer S21 Hyd (335Th)	Feb 2024	335 Th/s	5360 W	50 db	SHA-256	\$11.46 /day
 MicroBT WhatsMiner M63	Nov 2023	334 Th/s	6646 W	50 db	SHA-256	\$9.87 /day
 MicroBT WhatsMiner M66S	Nov 2023	298 Th/s	5513 W	50 db	SHA-256	\$9.30 /day
 MicroBT WhatsMiner M66	Nov 2023	280 Th/s	5572 W	50 db	SHA-256	\$8.27 /day
 Bitmain Antminer S21 Pro (234Th)	Jul 2024	234 Th/s	3531 W	75 db	SHA-256	\$8.26 /day
 Bitmain Antminer S19 XP Hyd (255Th)	Oct 2022	255 Th/s	5304 W	50 db	SHA-256	\$7.26 /day
 Bitmain Antminer S21 (200Th)	Feb 2024	200 Th/s	3550 W	75 db	SHA-256	\$6.48 /day
 Bitmain Antminer T19 Pro Hyd (235Th)	Feb 2024	235 Th/s	5170 W	30 db	SHA-256	\$6.35 /day
 Bitmain Antminer T21 (190Th)	Feb 2024	190 Th/s	3610 W	75 db	SHA-256	\$5.82 /day
 MicroBT WhatsMiner M60S	Feb 2024	186 Th/s	3441 W	75 db	SHA-256	\$5.81 /day
 MicroBT Whatsminer M53S	May 2023	260 Th/s	6760 W	50 db	SHA-256	\$5.78 /day
 MicroBT WhatsMiner M60	Feb 2024	172 Th/s	3422 W	75 db	SHA-256	\$5.08 /day
 MicroBT WhatsMiner M56S	Jan 2023	212 Th/s	5550 W	45 db	SHA-256	\$4.67 /day
 MicroBT Whatsminer M53	May 2023	230 Th/s	6670 W	50 db	SHA-256	\$4.28 /day
 MicroBT Whatsminer M33S++	Dec 2022	242 Th/s	7260 W	40 db	SHA-256	\$4.22 /day
 Canaan Avalon Made A1466	Sep 2023	150 Th/s	3230 W	75 db	SHA-256	\$4.14 /day
 Bitmain Antminer S19 Pro+ Hyd (198Th)	May 2022	198 Th/s	5445 W	50 db	SHA-256	\$4.04 /day
 Bitmain Antminer S19 XP (140Th)	Jul 2022	140 Th/s	3010 W	75 db	SHA-256	\$3.87 /day
 MicroBT WhatsMiner M56	Jan 2023	194 Th/s	5550 W	45 db	SHA-256	\$3.70 /day
 Bitmain Antminer S19k Pro (136Th)	Apr 2023	136 Th/s	3264 W	75 db	SHA-256	\$3.35 /day

Table 3. Most powerful and competitive mining rigs. Columns are model, announce date, hashrate, power consumption, noise level, SHA-256 is algorithm for Bitcoin, and gross profitability per day assuming 5 cents per kWh. Operating revenue after electricity costs only, ignoring equipment capital amortization. Source: asicminervalue.com

Difficulty of Mining

Bitcoin’s energy usage has risen rapidly over the past decade, but it seems to be flattening out somewhat. After all, the network is already highly secure due to the aggregate 600 Exahashes/second. And every four years there is a Halving (“halvening” or even “Halfinning” for Hal Finney) of the new bitcoin subsidy of the block reward. This is all preprogrammed in to happen each 210,000 blocks. At ten minutes average per block, that is a four-year cycle. So, the miners have to fight over a shrinking reward size. Fortunately for them, the price of Bitcoin has moved up strongly over the long term, although with high volatility.

You may wonder, how do the block sizes stay close to 10 minutes? This happens with fortnightly (each 2016 blocks) difficulty adjustments. If the block times are too quick on average, the difficulty of solving the cryptographic puzzle is increased by the ratio of 10 minutes to the average time, if they are too slow on average, the difficulty is decreased in a similar way. In general, difficulty rises as more and more hash rate has come into the Bitcoin mining industry through faster mining rigs and more machines deployed.

Figure 4 shows how steeply the difficulty has increased with time, as the 11th power of the Bitcoin blockchain’s age!

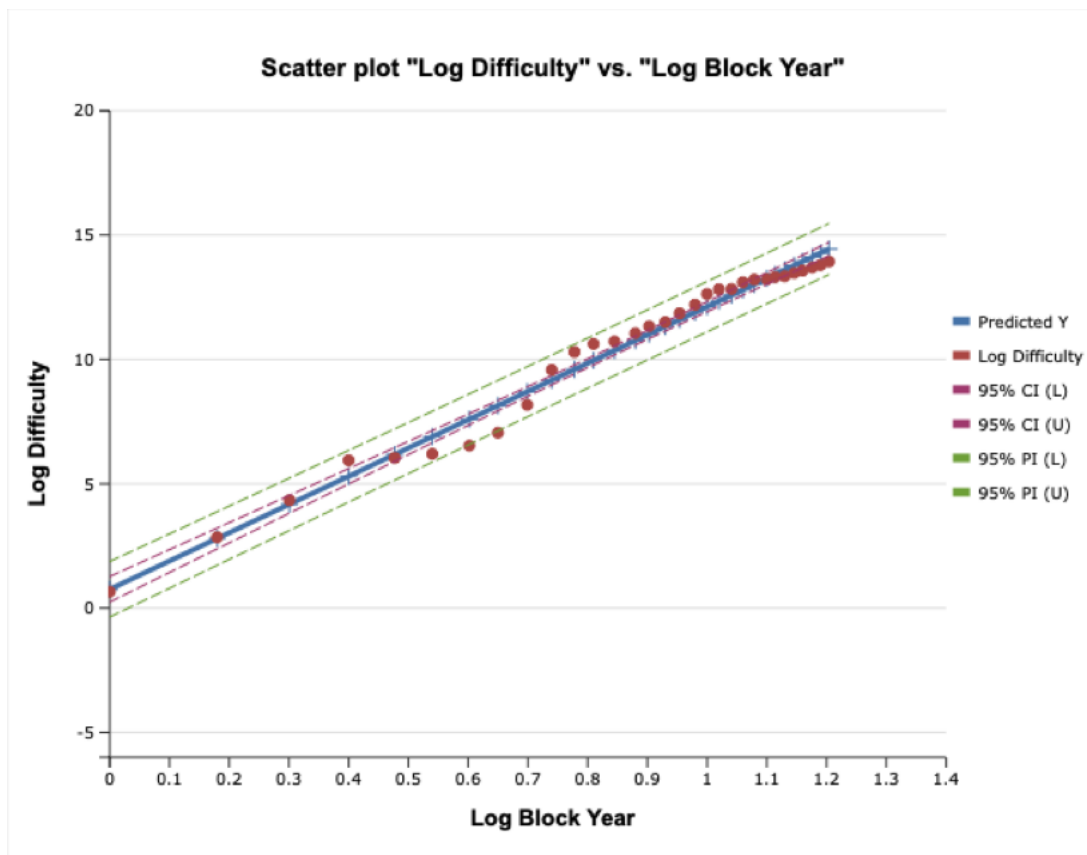


Figure 4. A log10-log10 chart of the difficulty parameter vs. time. The straight line indicates a power law, and the slope of the line indicates a very steep power law. This is a power law of index 11.3 with R² of 0.98, indicating a strong statistical result, and with a minimal uncertainty in the slope parameter of 0.3.

The difficulty parameter is a dimensionless parameter that is modified to keep block times close to 10 minutes. The time in seconds to find a block is basically Difficulty * 2³² / hashrate and the current difficulty is about 88 trillion. Thus, the long-term growth in hash rate is directly and linearly reflected in the difficulty parameter.

Publicly Traded Bitcoin Mining Companies

Company	Market Cap (Million \$)	Locations	Stock Price \$	Hash Rate installed Exahashes/sec ,self mining, (hosting)	Bitcoin Held in Treasury	Daily Bitcoin minted April 2024
Marathon Digital	4780	US, UAE, Paraguay	17.52	29.9	17,631	28.3
Clean Spark	3640	US	16.15	17.3	5,739	24.0
Riot Blockchain	3000	US	10.42	12.4	8,490	15.0
Cipher Mining	1220	US	4.14	7.7	2,033	10.0
Hut8 Mining	740	Canada	8.27	5.4 (31.3 services provision)	9,116	7.5
Bitdeer Technologies	670	US, Bhutan, Norway	5.74	6.7 (15.8 hosting, cloud offer)	0	10.0
Terawulf	660	US,	2.18	7.8	0	11.6
IREN (Iris Energy)	660	Canada, US	4.73	6.2	0	12.4
Bitfarms	600	Canada, US, Argentina	1.82	7.0	830	9.0
Core Scientific	590	US	3.35	20.4 (6.3)	n/a	9.9
Canaan	260	US, Kazakhstan, Ethiopia	0.88	2.1	909	~4
HIVE Blockchain	220	Canada, Sweden, Iceland	2.44	5.0	2,377	7.1
Totals	17,040			120.7 (53.4)	47,125	148.8

Table 4. The top publicly traded Bitcoin mining companies. Some of these companies have other business lines, such as AI/data center hosting, most are pure plays. In general, these are new businesses with significant venture capital invested and large capital expenses devoted to ramping up hashrate with new mining rigs, so although they may have good operating margins on mining, some are not profitable. Many of these are also keeping much of the Bitcoin they mine in their treasuries, collectively over \$3 billion in value. Data from companiesmarketcap.com and company web sites as of first 10 days of May 2024.

Table 4 shows the top 12 publicly traded Bitcoin mining companies. The Bitcoin mining business is extremely competitive, and the difficulty chart shows why. The aggregate global competition is growing exceptionally fast, the effective lifetime of ASIC-based mining equipment is relatively short, and the halvings provide regular downward pressure on the rewards. However the rapidly growing price provides an offset, and the most efficient businesses that seek out the lowest power costs can make money.

Businesses that have the lowest power costs, including load balancing subsidies with electric grid providers, and that have deep enough pockets to reinvest in new hardware aggressively, and yet can also hold onto a substantial fraction of minted Bitcoin in their treasuries, do best.

Following the time when China banned Bitcoin mining in 2021, many mining companies in the West raised capital in public markets to set up substantial operations. These publicly traded companies are based primarily in the US, Canada, Australia, and the UK, with their mining operations concentrated in the US and Canada. The top 12 have an aggregate market cap of \$17 billion and they collectively hold nearly 50,000 Bitcoin, around 1/4 of 1% of the extant supply.

Their aggregate hash rate is 120 Exahashes/second, which is 20% of the global hash rate. They also provide hosting and managed services for customers, an additional 53 Exahashes/s between the twelve, primarily provided by three companies and that takes the total hash rate provisioned by these twelve public companies to between 25% and 30% of the entire global hash rate.

Pre-halving Core Scientific and Riot Blockchain said that their operating costs to mine one Bitcoin were \$19,000 and \$23,000 respectively. Thus, post-halving their costs would be in the \$40,000 neighborhood since the block subsidy reward was cut in half from 6.25 BTC per block to 3.125 BTC in mid-April. This is to be compared to a Bitcoin price in the low \$60,000s but also in the favorable part of the four-year cycle that appears to have significant price rises in the year after each halving. The gross margin realized is required for equipment depreciation and capital investment in new systems, for any other unallocated costs, for profit, and to allow some minted Bitcoin to be held in the treasury to strengthen long-term balance sheets.

Pools are Brokers

Mining pools are just brokers of hash rate. They agglomerate hash rate from many sources and allow their members (customers) to share the rewards in proportion to their hash rate contribution to the pool. Many miners prefer to get smaller rewards on a more regular basis, since a single mining rig has less than a one in a million chance of winning any block reward. A million times ten minutes is 19 years, too long to wait. Odds are there would be several more halvings before you won a block. So, you point the hash rate toward a pool if you have only a few machines or even 100 machines, to smooth out returns.

The pools' influence on the market is indirect and miners can easily switch hash rate that is directed toward one pool to another. Pools charge brokerage fees ranging from under 1% to 4% depending on the broker and terms; in some cases, they keep the transaction fees portion of the block reward for themselves, in other cases they distribute to pool members.

Table 5 lists the top dozen pools and Foundry and AntPool continue to have the largest shares.

While mining pools are not necessarily miners themselves, they may own or manage affiliated crypto mining farms. On average, fees recently have accounted for about 10% of Bitcoin revenue to miners and brokered by pools, but they are quite variable. Ordinals, inscriptions, runes, and NFTs boost fee revenue. Interestingly, some blocks had fees larger than subsidy just at and after the fourth halving on 4/20/24 (UT). The overall domination of fees over subsidy for block rewards is probably a decade away if Bitcoin prices continue their overall power law growth.

Pool	Country	Bitcoin Hashrate Exahashes/s	% of all hashrate	Annual Run Rate \$M w/ 10% boost from fees
Foundry Digital	USA	167.3	26.6	3078
AntPool	Global	162.2	25.8	2985
ViaBTC	USA	78.3	12.5	1446
F2Pool	Global	62.5	9.9	1145
Binance	USA	28.2	4.5	520
Unknown	N/A	21.6	3.4	394
Luxor Tech	USA	18.2	2.9	336
Slushpool	Global	16.7	2.7	313
BTCdotcom	Global	13.3	2.1	243
SBI Crypto	Japan	12.8	2.0	231
SecPool	Global	8.3	1.2	139
Poolin	USA	7.5	1.2	139
Top 12 operators		580	95%	10,968
All Bitcoin Mining		620		11,571

Table 5. Top mining pools by value using Bitcoin price as of 5/6/24. Transaction fees add of order 10% (last 90-day average) on top of Bitcoin's block subsid reward.

Outlook for Mining Industry

The first point is that cryptocurrency mining will continue to be dominated by Bitcoin. The other alternative coins have faded for the most part and there is no clear challenger. Dogecoin has 1/60th of Bitcoin's market capitalization.

Hashrate has been growing at the 11th power of time; it may have slowed somewhat but is still growing at least as steeply as the 8th to 9th power of time. Price on the other hand grows at around the 5.5th power of Bitcoin's age. A mining company needs to plan for aggressive increases in hash power just to stay in place.

As the Bitcoin mining block subsidy is repeatedly cut every four years, at some point fees for processing transactions will have to exceed the revenue from minting new coins.

Given that Bitcoin price has followed a power law one can estimate when the transition could happen, and in this article, I predict it will be within two to three more halvings, by the middle of the next decade. By then the Bitcoin price should be high enough that 1% fees should be enough to reward the mining industry for their labors: <https://medium.com/thedarkside/bitcoin-mining-minting-or-transmitting-5c5cbae55af2>

On the power law curve the price could be three times higher at the next halving in 2028 and nine times or more by the 2032 halving. What is now 10% of revenue in the form of fees could then come to dominate in dollar terms over the block subsidy, which will be only 0.78 Bitcoin per block from 2032.

Whether the revenue to miners is from the block subsidy or fees, the miners with the most efficient operations including electricity cost, and deep enough pockets to reinvest continually in faster mining rigs, and yet hold some Bitcoin in their treasuries should have the best competitive positions. Some mining companies may continue to diversify their data centers to support AI and HPC application requirements to smooth out revenue during 'crypto winters'.

A wild card would be nation states starting to mine for strategic reasons, and they might even be willing to do so on a short-term loss basis.

5-1/2 Year Growth in Mining

Our first CryptoSuper500 report was five and a half years ago, in November 2018. While there are over 20,000 "cryptocurrencies" that have been created in the interval, only 52 of these coins including stable coins tied to fiat have valuations above \$2 billion. Most projects have been abandoned or are worth little; most were essentially get-rich quick schemes for their initiators. Only a small number of coins have used proof of work consensus algorithms; the ones that do not are more properly considered tokens.

Attribute	Nov. 2018	May 2024	5.5 Year Growth
Coins making cut for CryptoSuper report	Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Monero	Bitcoin, Dogecoin	Consolidation
Number of different cryptocurrencies	2000	Tens of thousands total	Majority abandoned, or worthless
Bitcoin Market Capitalization	\$111 billion	\$1260 billion	11.4 x
Bitcoin Price	\$6,334	\$64,000	10.1 x
Bitcoin annual production rate and fees	\$4.2 billion	\$11.6 billion	2.8 x
Bitcoin Hash Rate Exahash/s	57	600	10.5 x
Cryptocurrency Market Cap	\$220 billion	\$1312 billion	6.0 x
Top cryptos annual mining production w/ fees	\$5.6 billion	\$12.5 billion	2.2 x

Table 6. Key attributes of Bitcoin and major cryptocurrencies, comparing the first CryptoSuper report in 2018 with this report 5.5 years later. Bitcoin has been growing in value at a Moore's law-like rate, and its supercomputing crypto hashing power has been growing faster than Moore's law.

The Bitcoin market cap has grown in line with the 6th power of its age over this interval, one would have predicted growth by a factor of 12.5 and it grew quite close to that ratio. For price one would have predicted a factor of 10 and it grew by that same factor. Bitcoin annual production has grown by a smaller factor of 2.8 because there have been two halvings in the block subsidy during the past 5-1/2 years, in May 2020 and April 2024.

In the first report, coins other than Bitcoin contributed 1/4 of the annual production rate. In one prior report, Ethereum contributed as much as Bitcoin, but no longer. This is because Ethereum dropped out of the POW supercomputer mining contest; as a proof of stake coin, they now produce zero real economic value directly although many projects use their blockchain and smart contracts capability. Their network utility effect may accrue more dollar value for Ethereum, but it has been falling in value relative to Bitcoin since they abandoned proof of work over a year and a half ago.

In 2018 roughly 2/3 of mining hash rate was in China. Since the Chinese mining ban in May-June 2021 the US has quickly become the leading source of mining hash rate and of all hash rate over one quarter is due to venture funded startup mining companies with facilities primarily in North America.

The electricity input of Bitcoin was probably always greener than average due to hydropower in China in the past. And now due to solar, wind, nuclear, and hydro power sources in North America especially it is produced with more than 50% green or nuclear sourced power. (For the traditional finance industry this figure is 40%). Recently the focus has moved away from concerns about Bitcoin's electricity use toward a focus on the very large electricity requirements expected for AI data centers.

*“Bottom-up digital monies such as Bitcoin attempt to give the ledger back to the people, while top-down digital monies such as central bank digital currencies give nation states even more control over the ledger that people use.” - Lyn Alden, **Broken Money***

Comparison of Top500 Supercomputer List with Bitcoin Network

Frontier is the world's fastest supercomputer, with peak sustainable performance of 1.2 Exaflops/second. With the latest Top500 list released at the ISC conference of May 2024, the aggregate compute power of all the Top500 list is 8.2 Exaflops/second. One could combine all this computer power and not be able to compete with the Bitcoin hash power, since GPUs and CPUs are 100 to 1000 times slower for SHA-256 hashing purposes.

Bitcoin, a globally decentralized network of systems engaged in competition running the same core open-source software, is the world's fastest supercomputer for what it does, value creation.

As a gross estimate exercise, if one were to build out the current Bitcoin global hash power based only the latest high end Whatsminer 63S Hydro systems it would require 124,145 water cooled cabinets (located around the world) with a total weight of 95 megatons and a power requirement of 11 GigaWatts (GW). (The current average electricity consumption is uncertain but about 14 GW or 120 TeraWatt hours per annum.)

The cost would be \$13.3 billion (comparable in size to the global supercomputer market) for the systems that would produce \$11.6 billion of annual economic value with an electricity cost (at 4.5 cents per kWh average) of \$4.4 billion. If the equipment was written off on a four-year schedule (appropriate for one halving cycle) there would be \$3.3 billion of annual depreciation. The cash flow after electricity and depreciation would be \$3.9 billion as margin to cover other operational and facility costs, SG&A and profit, at the current Bitcoin price level. However, the out years might show less return depending on the relative rate of increase of prices and global hash rate.

The details for the Frontier supercomputer, the WhatsMiner Hydro systems configured 12 to a water-cooled rack, and for the equivalent number of cabinets for the entire Bitcoin network, are shown in Table 7.

Attribute	Frontier Supercomputer (#1)	Top 500 (all)	WhatsMiner 63S Hydro cabinet	Bitcoin Network Equivalent
Performance	1.2 Exaflops	8.2 Exaflops	4.68 Petahash/s	581 Exahash/s
One year increase	9%	57%	50% (vs. 53S)	57%
Chips	37,888 AMD Instinct GPUs 6nm; 9472 AMD Epyc CPUs	Hundreds of millions of cores	12 multithread, 5 nm ASIC	1,489,744 ASICs
Cabinets	74		1	124,145 cabinets
Power consumption	23 MegaWatts		89.2 KW	11,074 MW
Weight	296 tons		0.76 metric tons	94,600 metric tons
Cost	\$600 million		\$107,000	\$13.28 billion
Output	Science	Science & Engineering & AI	1.32 Bitcoin per year	164,250 Bitcoin per year
Value	Priceless	Enormous	\$93,400 per year	\$11.6 billion per year

Table 7. Comparison of a hypothetical Bitcoin network based on the latest high-end WhatsMiner 63S Hydro system, racked, with the Department of Energy's Frontier supercomputer and the Top 500 list. The cost to build out the global Bitcoin network is about 22 times that of the Frontier system while the economic output is measurable at \$11.6 billion per year currently. Since Bitcoin price increases as a power law, the value of this year's output should be worth substantially more in the future if the power law relation persists. Interestingly both the Top500 and the Bitcoin network have recently experienced a Moore's Law style growth rate of 57% per year.

Glossary

Bitcoin – The original cryptocurrency, blockchain and consensus algorithm was outlined in October 2008 in the Satoshi white paper. The Bitcoin blockchain began in January 2009. Bitcoin uses proof of work and has a disinflationary monetary policy based on Halvings.

Blockchain – A chain of transaction blocks with each block linked to the one prior and the one after by a hashing technique. Each block incorporates a hashed representation of the prior block along with its own transaction records. A specific type of database with time stamped and linked record blocks.

Block reward – The reward for being the winning miner of a block. It consists of a subsidy that is cut in half each 210,000 blocks, and any transaction fees collected by miners.

Block years – A block year is one quarter of a four-year Halving era of 210,000 blocks; block years have 52,500 blocks. They are close to a calendar year in duration, within a week or two. Over 14 block years have elapsed since Bitcoin began.

BTC – Abbreviation for the Bitcoin cryptocurrency.

Cryptocurrency – A currency stored in a digital ledger that implements cryptographic security to prevent theft or counterfeiting. Cryptocurrencies may be created with different mechanisms and the ledgers are often decentralized to varying degrees.

DeFi –Decentralized Finance. DeFi implements automated financial methods by use of cryptocurrencies and blockchains.

Dogecoin – A cryptocurrency created from Litecoin, itself a clone of Bitcoin, in 2013, as a joke. It has a mildly disinflationary monetary policy, but unlike Bitcoin, has no limit on the total supply.

ETH – The native cryptocurrency of the Ethereum network.

Ethereum – The second largest cryptocurrency by market value was created in 2015 by Vitalik Buterin, Joe Lubin and others. It was designed to implement smart contracts such as those used in DeFi. It shifted fully to proof of stake in September 2022, eliminating the former usage of a proof of work mining algorithm.

Halvings – The algorithmically enforced decrease in the block reward subsidy for Bitcoin miners. Originally this was 50 BTC for the winning block. Halvings occur roughly four years apart after each interval of 210,000 blocks. The last halving in May 2020 dropped the subsidy from 12.5 to 6.25 bitcoins per block, the next will be around April 2024.

Hash rate – The rate at which a computer system (mining rig) can generate hash guesses to solve the cryptographic puzzle. A Terahash/s is a trillion hashes per second, a Petahash/s is a quadrillion, and an Exahash/s is a quintillion (10^{18}) hashes per second. A Zettahash/s is one thousand Exahash/s.

Lightning – Lightning is a second layer solution for Bitcoin that allows for speedy payments including for very small amounts at very low cost. Lightning channels are opened between parties, and this forms a network. Lightning payments are eventually resolved back onto the first level blockchain in batched transactions.

Miners – The computer systems that solve the cryptographic puzzle for a proof of work cryptocurrency. Miners are characterized by hash rate, the amount of solution power. Custom ASICs or GPUs are employed, typically. The first computer that solves the puzzle commits the block of transactions and receives the block reward. Miners are minterers of cryptocurrency, through the combination of electricity, cryptographic hashing cycles, and a proof of work lottery reward system.

Minting – Bitcoin and other proof of work coins are in fact minted, not mined. Nothing is dug up, and new coins are minted with each block according to the consensus algorithm which in effect enacts a monetary policy.

Money – A medium of exchange, store of value, and unit of account. Bitcoin represents monetary technology; it has not achieved full 'moneyness' but is on the path as utility grows. Ethereum removed proof of work and that makes it less 'money' and more of a payments and decentralized finance solution. Bitcoin is now legal tender alongside existing currencies as money in the countries of El Salvador and the Central African Republic.

Pools – Pools aggregate hash rate from mining farms plus smaller miners, that choose to contribute their hash power into a collective pool, in order to gain a proportionate share of the pool's mining rewards. Pools are essentially brokerages, run by companies for a fee share of the Bitcoin processed. They are not themselves mining operations, although they may have associated mining farm businesses.

Proof of Stake – In proof of stake, rewards or dividends are paid, in proportional to their share, to existing holders of a coin or token, who have governance and block validator privileges. Holding such a token is conceptually similar to holding a share of a company. Long term value depends on scarcity and utility, but security is much lower than with proof of work.

Proof of Work – In proof of work, a cryptographic lottery must be won by miners competing with their hash power. The winning miner validates the transactions for a particular block and receives a block reward that includes a subsidy of new coins and transaction fees. Monetary policy is set by changing the block subsidy on a schedule, and a difficulty adjustment keeps block times around the nominal target. Proof of work and storage on a decentralized ledger with many copies solves the double spending (of the same coin) and counterfeiting problems.

Reusable Proof of Work - Hal Finney created the last key technological improvement required for Bitcoin, with a concept for making proof of work tokens reusable. This means they can be spent repeatedly by their new owners, like a coin, rather than used once, like a postage stamp.

Smart contract – An automated contract for exchange of value implementing agreed upon rules between the parties for transfers.

Time Chain – See blockchain. Blockchains are chains of time-stamped transactions, laid out as a permanent temporal record of those transactions.

References, Data Sources

<https://21lessons.com/> - by Gigi, free online book on Bitcoin

<https://www.asicminervalue.com/> - list of top mining rigs and profitability

<https://bitcoinminingcouncil.com/bitcoin-mining-electricity-mix-increased-to-59-5-sustainable-in-q2-2022/> - Bitcoin Mining Council estimate of 'greenness' of electricity input

Broken Money, Lyn Alden 2023, Timestamp Press

<https://www.btcpolicy.org/articles/great-power-network-competition-bitcoin> - Matthew Pines 2023, "Great Power Network Competition and Bitcoin"

<https://ccaf.io/cbnsi/cbeci> - Cambridge Centre for Alternative Finance Bitcoin energy statistics

<https://www.cfr.org/backgroundunder/dollar-worlds-reserve-currency> - Council on Foreign Relations, 2023. Discusses why the dollar remains the world's reserve currency for the foreseeable future.

CoinMarketCap.com - market cap for most cryptocurrencies

coinwarz.com - profit margins for Bitcoin mining hardware

companiesmarketcap.com - market prices and capitalization for largest companies and gold, silver, Bitcoin

<https://www.ecb.europa.eu/press/pr/date/2023/html/ecb.pr231018~111a014ae7.en.html> ECB statement on CBDC possibility

<https://www.educative.io/answers/what-are-the-different-steps-in-sha-256> - SHA-256 algorithm details

<https://ember-climate.org/insights/research/global-electricity-review-2023/> - Electricity review 2023 from Ember

<https://studio.glassnode.com/dashboards/btc-miners> - Glassnode, mining metrics

<https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp> - Why does Bitcoin have value?

<https://medium.com/the-capital/aristotle-would-prefer-bitcoin-f0f825f87d3f> - Aristotle would approve of Bitcoin

<https://medium.com/@cryptoassets0417/tenth-cryptosuper500-report-72f66ee20850> - Tenth CryptoSuper 500 report June 2023

Miningpoolstats.stream - tracks hash rate for mined coins and larger mining pools

<https://www.educative.io/answers/what-are-the-different-steps-in-sha-256> - SHA-256 algorithm details

Softwar, Jason Lowery 2023, MIT master's thesis, no longer available on Amazon due to Pentagon embargo

Please visit OrionX.net/research for additional information and related reports.

Copyright notice: This document may not be reproduced or transmitted in any form or by any means without prior written permission from the publisher. All trademarks and registered trademarks of the products and corporations mentioned are the property of the respective holders. The information contained in this publication has been obtained from sources believed to be reliable. OrionX does not warrant the completeness, accuracy, or adequacy of this report and bears no liability for errors, omissions, inadequacies, or interpretations of the information contained herein. Opinions reflect the judgment of OrionX at the time of publication and are subject to change without notice.