OrionX¹

The OrionX Constellation Blockchain

Thirteenth CryptoSuper 500 Report

Sixth anniversary report on a \$15 billion industry

Stephen Perrenod

November 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 Coinbase, MicroStrategy, Semler Scientific and Bitcoin ETPs but no positions in Bitcoin mining stocks.

"Newton practiced alchemy without result, and also ran the British mint. He would have been fascinated by Bitcoin. In a single 10-minute block we have mining, assaying, minting, and transmitting of value, simultaneously. Raw energy, powerful math, and game theory are the alchemy at work over a global supercomputing network" - @moneyordebt

Evolution

Market Update

As this report was in final editing, Bitcoin's priced surged to nearly \$90,000 from the \$75,000 price range used in the third revision of the report. If this price area holds up then the annual economic value is close to 20% higher than what is tabulated herein and is approximately \$15 billions of Bitcoin production per year.

Preface

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.

As I complete this, the Presidential and Congressional elections were held earlier this week and Bitcoin's price jumped significantly to above \$75,000 at the prospects of friendlier crypto policies from a Trump administration and the possibility of the US government establishing a strategic reserve holding substantial Bitcoin. Currently the US government owns the most of any government, about 1%, from coins seized from criminal activities. In the past these have been auctioned off, but may now form the initial component of such a strategic reserve.

We are just past the 16th anniversary of Satoshi Nakamoto's publication of the Bitcoin white paper on October 31, 2008. The blockchain went live on January 3, 2009. The first trades of Bitcoin valued it at a fraction of a penny, now it is priced at \$75,000 having scaled in value by over 7 orders of magnitude. Many people do not know that Bitcoin is divisible into much smaller units, 100 million Sats per Bitcoin, now somewhat over 1000 Sats per dollar, so although the supply is fixed at 21 million, it is very scalable as its price increases since that supply is also equals to 2.1 quadrillion Sats. In this way, very high value amounts and modest amounts can be denominated.

Figure 1. Bitcoin's prehistory spans 40 years. The final key technology building block was Hal Finney's modification of proof of work to make bitcoins reusable, four years before the Bitcoin white paper was published on Halloween, 2008.

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

OrionX^a



Bitcoin prehistory - It's the result of 40 years of research, development and demand

Overview

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 fourth halving of Bitcoin block rewards was on April 19, 2024 (US time), a month prior to our <u>last report</u>. And the price of Bitcoin has been relatively flat since then.

This has put some pressure on Bitcoin mining companies, and most of the publicly traded companies have now implemented or announced expansion to their business strategies to include hosting of HPC and AI workloads. This will potentially provide them with more certainty for a portion of their revenue, given Bitcoin's high volatility and quasi-periodic booms and busts.

Bitcoin minting continues to produce about \$12 billion in annual economic value. It is unrivaled by other proof-ofwork cryptocurrencies. Only one other, Dogecoin, makes the cut for this report, and it is only a small fraction of Bitcoin's production value. Ethereum once rivaled Bitcoin for value minted but gave up the race when it switched to proof-of-stake. Litecoin, Bitcoin Cash (a clone with a much lower hash rate and value), Ethereum Classic, Monero, and a newly popular Kaspa, all fail to make the cut of \$250 million minimum annual production.

Institutional and corporate adoption

Over 10 ETPs (similar to ETFs) for Bitcoin were approved in early 2024, and they have grown substantially in holdings, reaching almost 1 million Bitcoin in total. Exchanges such as Coinbase, Finance, and Bitfinex hold over 3 million Bitcoin.

In addition to ETFs, exchanges and Bitcoin mining companies, a few other corporations and private companies have added Bitcoin to their balance sheet, most notably MicroStrategy, which has accumulated over 1% of all

OrionX

The OrionX Constellation Blockchain

Bitcoin, and shows no sign of slowing down. In fact they just announced plans for \$42 billion of equity and convertible debt issuance over the next three years in order to acquire additional Bitcoin for their treasury. Tesla has held Bitcoin for some time. The largest private company holders are BlockOne, a Chinese company, and Tether, the producer of the largest dollar linked stablecoin. The FASB accounting rules have been modified in a manner that makes it now easier for companies to keep Bitcoin on their balance sheets.

Very recently an initiative was placed on the agenda, for a vote at Microsoft's annual meeting, to study the possibility of adding Bitcoin to their treasury. Management has recommended a no vote on the proposal, but some of the big holders such as Blackrock may vote for it.

Several sovereign wealth funds, including in Singapore and the UAE, have added Bitcoin to their portfolios and we are seeing some early adoption of Bitcoin on state and local pension fund balance sheets in the US as well.

The US, China, UK, Ukraine and Bhutan governments in total hold about half a million Bitcoin from seizures, donations, and mining.

More broadly, there are one million addresses that contain at least one Bitcoin, and 52 million addresses holding some nonzero amount of Bitcoin.

Politics and geopolitics

The SEC was essentially forced by a court finding in late 2023 to open the door for ETFs to be approved for trading, and nearly a dozen (ETPs, to be precise) began acquiring Bitcoin and trading their shares in early 2024

Two presidential candidates, Trump and RFK Jr., called for a Bitcoin reserve position to be created by the US government, and Senator Cynthia Lummis of Wyoming has introduced a bill to this effect. The bill would empower the Treasury Secretary to convert some of the gold holding of the US to Bitcoin and authorize purchase of up to one million Bitcoin over a 5 year period. The Bitcoin strategic reserve could begin with the 200,000 plus Bitcoin currently held by the US Marshals Service from various seizures.

There is a new research paper at the European Central Bank on the topic of Bitcoin; the authors are worried that it will keep rising in price and thereby impoverish society at large, and they call for regulation to control the price of Bitcoin in the Eurozone. This is a non-starter for a globally traded asset, and Bitcoin has to gain more than an order of magnitude in value in order to match gold, which has not yet impoverished Europe despite Europe having plundered large amounts from its colonies in the past. The European Central Bank is also serious about launching a CBDC, central bank digital currency, and Bitcoin is seen as competition, and explains much of the motivation.

The Federal Reserve has made no decision in regard to a CBDC. But the Minneapolis Fed called Bitcoin 'useless paper', an ironic statement for an organization that issues Federal Reserve notes as paper currency, and suggested it should be banned. China has a CBDC implemented, but progress in its roll out the past few years has been slow.

The BIS, the central banker's central bank, has deprecated Bitcoin from a Basel equity capital requirement perspective. As an end run around this position, the Swiss National Bank has reportedly purchased Microstrategy stock instead.

In most countries it is legal to own Bitcoin, and the authorities are mainly concerned about KYC (know your customer) and AML (anti money-laundering). Since there have been a number of high profile exchange failures

OrionX a

The OrionX Constellation Blockchain

(Mt. Gox and FTX are two of the best known failures), authorities have put better controls in place. Governments want to be able to monitor international transfers in Bitcoin and monitor and tax realized capital gains.

Bitcoin mining is brutally competitive



Figure 2. The rise of Bitcoin difficulty plotted as log difficulty versus log age (log10, age in days). On a log-log plot a straight line indicates a power law relationship. Bitcoin's difficulty of mining is linearly proportional to the aggregate global hash rate, which has grown incredibly fast, due to faster ASICs and more mining rigs, essentially as the 12th power of Bitcoin's age. It may be flattening somewhat in recent years.

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 700 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 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.

The above figure shows this steep power rise in the difficulty parameter for the Nakamoto consensus protocol that implements a winner take all lottery. The difficulty is re-evaluated about every two weeks (2016 blocks) in order to keep block times close to 10 minutes. Over the full history the difficulty, which is linearly proportional to the smoothed, global, aggregate hash rate, has risen as the age of Bitcoin to the 12th power!

Fortunately for miners, Bitcoin increases in price long-term at nearly the sixth power (the square of the cube) of its age. But unfortunately for miners, the competition is brutal, with the difficulty of solving the puzzle for the block reward growing as the square of that. There is some indication that the rise in hash rate has slowed to perhaps the ninth power of time, but it remains steeper even than the rapid rise in price.

Liquid cooling becoming ubiquitous

The table below shows 22 of the fastest mining rigs on the market, ranging from 200 Terahashes/s (TH/s) up to 860 TH/s (shipping by year end), and with power input ranging from 3.4 kiloWatts up to 11.1 kiloWatts. Most of the systems high on this list use hydro cooling or immersion cooling as a consequence of high power density.

Two Chinese companies continue to dominate the list, with their ASICs sourced from TMSC and Samsung for the Bitmain and MicroBT product families, respectively.

Model o	Release 0	Hashrate :	Power o	Noise o	Тор о	Algorithm 0	Profit \downarrow
Bitmain Antminer S21e XP Hyd 3U	Dec 2024	860 Th/s	11180 w	50 db	₿	SHA-256	\$36.34 /day
Bitmain Antminer S21 XP Hyd (473Th)	Nov 2024	473 Th/s	5676 w	50 db	B	SHA-256	\$20.55 /day
Bitdeer SealMiner A2 Hyd	Dec 2024	446 Th/s	7360 w	50 db	B	SHA-256	\$16.97 /day
WhatsMiner M63S	Nov 2023	390 Th/s	7215 w	50 db	₿	SHA-256	\$13.90 /day
Bitmain Antminer S21 Hyd (335Th)	Feb 2024	335 Th/s	5360 w	50 db	₿	SHA-256	\$12.95 /day
Bitmain Antminer S21+ Hyd (319Th)	Feb 2025	319 Th/s	4785 w	50 db	B	SHA-256	\$12.71 /day
Bitmain Antminer S21 XP Immersion (300Th)	Oct 2024	300 Th/s	4050 w	50 db	B	SHA-256	\$12.50 /day
MicroBT WhatsMiner M63	Nov 2023	334 Th/s	6646 w	50 db	₿	SHA-256	\$11.35 /day
Bitmain Antminer S21 XP (270Th)	Oct 2024	270 Th/s	3645 w	75 db	₿	SHA-256	\$11.25 /day
MicroBT WhatsMiner M66S	Nov 2023	298 Th/s	5513 w	50 db	₿	SHA-256	\$10.62 /day
MicroBT WhatsMiner M66	Nov 2023	280 Th/s	5572 w	50 db	₿	SHA-256	\$9.51/day
Bitmain Antminer S21 Pro (234Th)	Jul 2024	234 Th/s	3531 w	75 db	₿	SHA-256	\$9.30 /day
Canaan Avalon A1566I	Jul 2024	249 Th/s	4500 w	50 db	B	SHA-256	\$9.00 /day
Bitdeer SealMiner A2	Dec 2024	226 Th/s	3730 w	75 db	₿	SHA-256	\$8.60 /day
Bitmain Antminer S19 XP Hyd (255Th)	Oct 2022	255 Th/s	5304 w	50 db	₿	SHA-256	\$8.39 /day
Bitmain Antminer S21+ (216Th)	Feb 2025	216 Th/s	3564 w	75 db	₿	SHA-256	\$8.22 /day
MicroBT WhatsMiner M60S+	Aug 2024	212 Th/s	3600 w	75 db	₿	SHA-256	\$7.94 /day
Bitmain Antminer T19 Pro Hyd (235Th)	Feb 2024	235 Th/s	5170 w	30 db	₿	SHA-256	\$7.39 /day
Bitmain Antminer S21 (200Th)	Feb 2024	200 Th/s	3550 w	75 db	₿	SHA-256	\$7.37 /day
MicroBT Whatsminer M53S	May 2023	260 Th/s	6760 w	50 db	₿	SHA-256	\$6.93 /day
Bitmain Antminer T21 (190Th)	Feb 2024	190 Th/s	3610 w	75 db	B	SHA-256	\$6.66 /day
MicroBT WhatsMiner M60S	Feb 2024	186 Th/s	3441 w	75 db	₿	SHA-256	\$6.63 /day

Table 1. The columns in this mining rig table are model name, release date, hashrate, power consumption, noise level, SHA-256 is algorithm for Bitcoin, and gross profitability per day at 5 cents per kWh. This is operating revenue after electricity costs only, ignoring equipment capital amortization. Source: <u>asicminervalue.com</u> as of 11/7/24.

As a rough illustration of the scale of the global decentralized supercomputer mining network, if we derived all of the hash rate from identical Whatsminer M63S models, for example, it would require close to 2 million systems, or 160,000 cabinets, drawing 14 GigaWatts of power. But that power also creates over \$12 billion of new economic value per year, it is not one-time consumption, but production of permanent value.

Proof of Work (POW)

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 requires

OrionX E

substantial computational power and electrical power input to create the asset in question. And POW underpins security substantially as well as value. We looked at all POW coins above \$2 billion in market cap but only two made the cut of \$250 million annual value production. Table 2 shows attributes of those two coins.

Coin	Market Cap (B\$)	Total hash rate and Algorithm	Annual Production rate \$B (nominal)	Current Supply (millions)	Max Supply (millions)
Bitcoin	1480	750 Exa, SHA-256	12.6	19.77	21
Dogecoin	28	1200 Tera, Scrypt	1.0	146,600	infinite

Table 2. The first three columns give the coin name, its market cap as of 11/7/2024, and its cryptographic hash algorithm rate and type. The next three columns give the annual production value and the current and maximum supply. Only Bitcoin is in the hundreds of Exahashes/sec, and due to that and first mover advantage, nearly all the economic value is in Bitcoin.

The highest hash rate by far is Bitcoin's 700 Exahashes/second (600 billion billion). The number two mined coin by annual value is Dogecoin with around 1 Petahash/s, which is a factor of 600,000 lower, although it is not an apple- to-apples comparison. The two use different algorithms, SHA-256 hashing for Bitcoin and a less compute intensive Scrypt in the case of Dogecoin. While the two hashrates are not directly comparable, the relative value of the two networks is. And Bitcoin is 50 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 of systems; it is not at the same scale.

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. Bitcoin as the original, the 'real thing', has by far the deepest moat.

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

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.

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

OrionX a

The OrionX Constellation Blockchain

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 hyperscalers 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 3. 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.

OrionX m

Power consumption of Bitcoin mining

According to the <u>Cambridge Centre for Alternative Finance</u> (CCAF) the current Bitcoin power consumption globally is around 19 GigaWatts.

Bitcoin has often been attacked for its high power consumption, indeed it consumes around 1/2 to 2/3 of 1% of global electricity, about equal to the country of Egypt. But this is only 0.16% - 0.26% by various estimates, of all global energy, and its share of CO2e emissions has been estimated by the Bitcoin Mining Council as just 0.11%

Bitcoin preferentially seeks out low-cost sources of electricity and is able to tolerate more intermittent sources including solar, wind, and hydroelectric power. It also is easily shut in or cut back if the grid is experiencing peak demand. Among the members of the Bitcoin Mining Council, 60% of their electricity usage is carbon neutral.

In addition, Bitcoin mining is now being used to capture methane that would otherwise be flared or even vented, and methane is 25 to 80 times as bad as CO2 for global warming. Global gas flaring alone could cover Bitcoin's power needs several times over, according to the CCAF.

Furthermore, unlike most electricity usage such as lighting, appliances, and Tesla charging, that are one-time consumption activities, mining Bitcoin is a production process, not a consumption process

Only the transaction fees portion of the block reward is consumption and that is currently around 2%. A full 98% of the electricity is directed toward production of permanent reusable value, in the form of new Bitcoin minting, just as if one were minting gold coins that can be used over and over and retain and grow their value.

Bitcoin mining is no longer the chief bogeyman for electrical consumption, that honor is now moving to data centers broadly. And most data center electricity usage is not for production processes but for consumption; that includes AI model execution, for example.

The Electric Power Research Institute estimates that data center usage of electricity <u>may rise to 9% of the total</u> <u>supply of electricity in the US by 2030</u>.

Public companies are the leading edge

The most rapid growth of mining hash rate is with publicly traded VC-funded companies, especially since the Chinese crackdown of 2021 on Bitcoin mining. In aggregate, the top companies in the space have a market cap of \$26 billion. They also hold around 62,000 Bitcoins in their corporate treasuries.

Table 3 below shows the market cap, Bitcoin holdings, and other information on the top 13 public companies. We also note whether HPC/AI offerings are part of their portfolio. Collectively these public companies are now responsible for nearly one quarter of all Bitcoin production. They are headquartered in four countries: the US, Canada, Singapore, and Australia, and all trade in New York as well as their home countries.

Their average reported cost of power is well below 5 cents per kiloWatt-hour (kWh). The top four consume over 1/2 of a GigaWatt each. Overall though, due to increased efficiency of miners, the total power utilized by the network has been climbing more gradually during the last two years than previously.

OrionX

The OrionX Constellation Blockchain

Symbol	Company Name	Share Price (\$)	Market Cap (B\$)	Bitcoin Holdings	Expansion plans	HPC/AI Current or Planned	Other
BITF	Bitfarms	1.97	0.95	1,147	+10 EH YE 24	Ν	4 countries including South America, 12 DC
BTDR	Bitdeer Technologies	7.72	1.37	~370	2.5 GigaWatts by 2026	Y	3 countries including Bhutan, Norway, 6 DC, 67% Carbon free
CAN	Canaan	0.97	0.29	1,114	Modest	Y, Al chip	Mining rig manufacturer; 5 countries, 8 DCs, Ethiopia, \$.042 per kWh ave.
CIFR	Cipher Mining Tech.	5.15	1.84	2,270	Double to 566 MW in 2025	Υ	\$.027 per kWh, electricity per BTC ~\$26K
CLSK	CleanSpark	11.63	3.10	8,049	50 EH/s during 2025 (up from 30)	Ν	Recent 200% growth rate in Hashpower year-on-year
CORZ	Core Scientific	13.52	3.54	0	750 MW expansion by 2028 shift to HPC	Y	\$.045 per KWh
FUFU	Bit FuFu	4.77	0.78			Ν	100% year-on-year revenue growth, adding facility in Ethiopia
HIVE	Hive Digital Tech.	3.65	0.43	2,604	100 MW, goal double hashrate	Y	Northern Europe
HUT	Hut8	15.11	1.41	9,106		Y	15 Bitcoin and DC sites, \$.032 per KWh
IREN	IREN	8.68	1.64		1 GigaWatt addition	Y, 10% revenue	100% renewable
MARA	MARA Holdings	18.88	5.56	26,842	Over 50 EH/s during 2025	Y	4 continents, 14 DCs, stranded energy focus
RIOT	Riot Platforms	9.77	2.97	10,427	2 GigaWatts expansion to 100 EH/s by 2027	Ν	Power cost \$.027 per kWh, 62% GM, direct costs \$25K per BTC
WULF	Terawulf	6.40	2.45		300 MW additional by end 2025	Y	91% Zero Carbon, \$.035 kWh
Total			26.33	61,929		69%	

OrionX

The OrionX Constellation Blockchain

Table 3. Publicly traded mining companies with \$300 million or higher market capitalization. The combined market cap is \$26 billion and they are responsible for about 23% of all Bitcoin production. Of the 13 companies, 8 have added HPC/AI hosting services to their business strategies. Four of the companies are consuming over 1/2 a GigaWatt of electricity each. Their average power costs are below 5 cents per kWh.



Figure 4. The number of Bitcoin mined by each of the top 14 publicly traded miners during the month of September, compiled by Compass Mining. Each 450 Bitcoin is approximately one day's worth of all Bitcoin mined, so almost exactly a week's worth of all Bitcoin production globally is represented here, consistent with a 23% share of all mining at these 14 companies, as of 10/24/24.

Businesses that have the lowest power costs, including load balancing subsidies from 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.

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;

OrionX^{te}

in some cases, they keep the transaction fees portion of the block reward for themselves, in other cases they distribute to pool members.

Table 4 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 2% of Bitcoin revenue to miners and brokered by pools, but they are quite variable. Ordinals, inscriptions, runes, and NFTs boost fee revenue. 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	# Winning Blocks in a month	Annual Run Rate \$M w/ 2% boost from fees
Foundry Digital	USA	196.7	1210	3123
AntPool	China	173.1	1065	2753
ViaBTC	China	93.8	577	1491
F2Pool	China	69.7	429	1113
MARA	USA	30.1	185	479
Binance	China	20.2	124	321
SpiderPool	China	17.9	110	284
Luxor	USA	12	74	191
BraiinsPool	Czech	11.2	69	178
SecPool	China	9.3	57	147
BTCdotcom	China	7.8	48	124
SBICrypto	Japan	5.2	32	83
Top 12 operators		647	97%	10,290
All Bitcoin Mining		670		10,650

OrionX^E

Table 4. Top mining pools by value using Bitcoin price of \$67,000 as of 10/24/24. Transaction fees add of order 2% currently 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 1/50th of Bitcoin's market capitalization.

Hashrate has been growing at the 11th to 12th 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 5.7th 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-mining-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 diversity 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.

Trends over 6 years

Table 5 below shows the growth rate of various metrics over the six-year interval since our first CryptoSuper report. There has been continued consolidation around Bitcoin as the premier coin, with now only one other coin making the cut and it, Dogecoin, contributes just 7% of the annual economic value.

Over this interval there has been an increase in market cap from \$100 billion to \$1.5 trillion for Bitcoin, up by a factor of 13 as the price increased and supply also increased slightly. The annual production rate in economic value for Bitcoin has increased by close to a factor of 3, to \$12.6 billion. The hash rate has increased roughly in line with the price, by a factor of 12.

The outlook for the next year is higher Bitcoin prices and better margins for miners, as we are in the favorable portion of Bitcoin's quasi-periodic behavior with a four-year cycle. The global liquidity backdrop also appears favorable.

OrionX a

Attribute	Nov. 2018	Nov. 2024	6 Year Growth
Coins making cut for CryptoSuper report	Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Monero	Bitcoin, Dogecoin	Consolidation
Number of different cryptocurrencies	2000	~ 10,000 active	Vast Majority worth little
Bitcoin Market Capitalization	\$111 billion	\$1480 billion	13 x
Bitcoin Price	\$6,334	\$75,000	12 x
Bitcoin annual production rate	\$4.2 billion	\$12.6 billion	3 x
Bitcoin Hash Rate Exahash/s	tcoin Hash Rate 57 xahash/s		12 x
Cryptocurrency Market Cap	\$220 billion	\$2470 billion	11 x
Top cryptos annual mining production w/ fees	\$5.6 billion	\$13.6 billion	2.4 x

Table 5. Metrics comparing Bitcoin and mined crypto business growth during the past six years. The Bitcoin production value has increased a factor of three as the price increased a factor of 12. The reason for the still high, but much slower relative increase in production value, is of course the two halvings of Bitcoin reward subsidies in May 2020 and April 2024. These are intrinsic to the Nakamoto consensus algorithm, to enforce the absolutely limited and finite supply cap of 21 million Bitcoin.

"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**

OrionX m

APPENDIX: 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 prior 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 coopetition 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 150,000 water cooled cabinets (located around the world) with a total weight of 104 megatons and a power requirement of 13 GigaWatts (GW). (The current average electricity consumption is uncertain but about 19 GW.)

The cost would be \$14.6 billion (comparable in size to the global supercomputer hardware market) for the systems that would produce \$12 billion of annual economic value with an electricity cost (at 4.5 cents per kWh average) of nearly \$5 billion. If the equipment was written off on a four-year schedule (appropriate for one halving cycle) there would be \$3.7 billion of annual depreciation.

Attribute	Frontier Supercomputer (#1)	Top 500 (all) May 2024	WhatsMiner 63S Hydro cabinet	Bitcoin Network Equivalent
Performance	1.2 Exaflops	8.2 Exaflops	4.68 Petahash/s	700 Exahash/s
One year increase	9%	57%	~60% for industry	65%
Chips	37,888 AMD Instinct GPUS 6nm; 9472 AMD Epyc CPUs	Hundreds of millons of cores	12 multithread, 5 nm ASIC	1,795,000 ASICs
Cabinets	74		1	150,000 cabinets
Power consumption	23 MegaWatts		89.2 KW	13,340 MW
Weight	296 tons		0.76 metric tons	103,823 metric tons
Cost	\$600 million		\$107,000	\$14.62 billion
Output	Science	Science & Engineering & Al	1.12 Bitcoin per year	164,000 Bitcoin per year
Value	Priceless	Enormous	\$70,600 per year	\$12.3 billion per year

Table 6. 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 \$12.3 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.

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 minters of cryptocurrency, through the combination of electricity, cryptographic hashing cycles, and a proof of work lottery reward system.

OrionX^z

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.

OrionX m

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

<u>https://www.cfr.org/backgrounder/dollar-worlds-reserve-currency</u> - 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.