OrionX.net

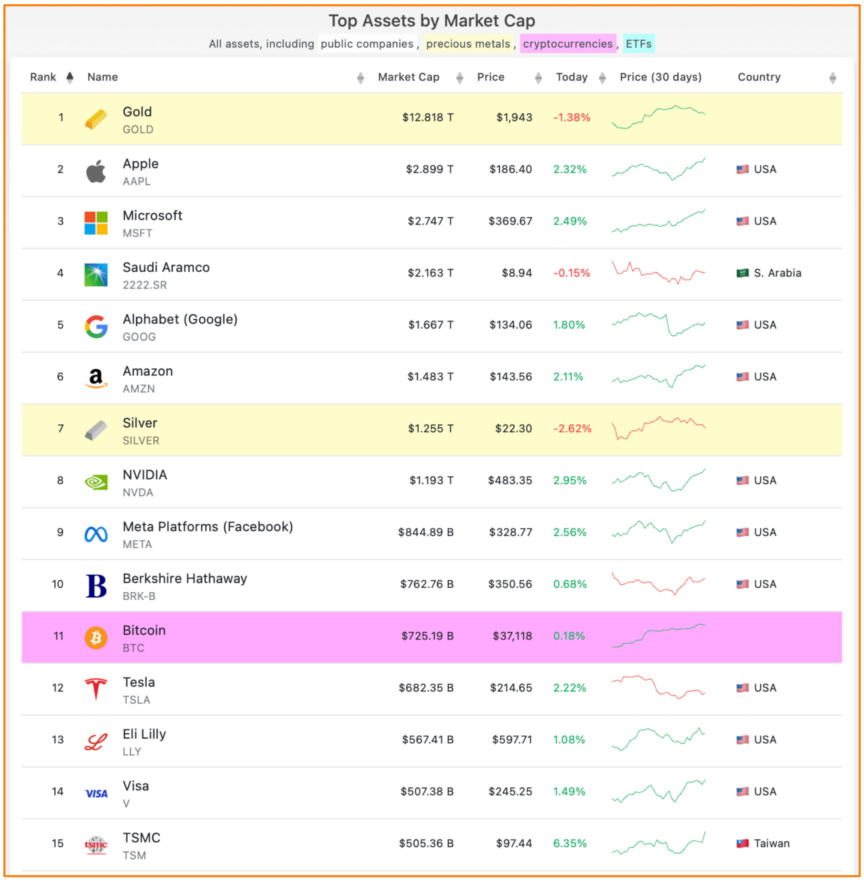
Evolution

The OrionX Constellation
Blockchain

Eleventh CryptoSuper 500 List
Bitcoin Mining Approaching its Zettahash Era

Stephen Perrenod
November 2023

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, Cipher Mining, Hut8, Marathon, and ETF-like vehicles GBTC and BITO that hold Bitcoin and its futures contracts.



Top Assets by Market Cap

All assets, including public companies, precious metals, cryptocurrencies, ETFs

Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	Gold GOLD	$12.818 T	$1,943	-1.38%		
2	Apple AAPL	$2.899 T	$186.40	2.32%		USA
3	Microsoft MSFT	$2.747 T	$369.67	2.49%		USA
4	Saudi Aramco 2222.SR	$2.163 T	$8.94	-0.15%		S. Arabia
5	Alphabet (Google) GOOG	$1.667 T	$134.06	1.80%		USA
6	Amazon AMZN	$1.483 T	$143.56	2.11%		USA
7	Silver SILVER	$1.255 T	$22.30	-2.62%		
8	NVIDIA NVDA	$1.193 T	$483.35	2.95%		USA
9	Meta Platforms (Facebook) META	$844.89 B	$328.77	2.56%		USA
10	Berkshire Hathaway BRK-B	$762.76 B	$350.56	0.68%		USA
11	Bitcoin BTC	$725.19 B	$37,118	0.18%		
12	Tesla TSLA	$682.35 B	$214.65	2.22%		USA
13	Eli Lilly LLY	$567.41 B	$597.71	1.08%		USA
14	Visa V	$507.38 B	$245.25	1.49%		USA
15	TSMC TSM	$505.36 B	$97.44	6.35%		Taiwan

Table 1. Top assets by market capitalization as of 12 November 2023. Twelve of these are the world's most valuable companies, while three are the most valuable assets with a monetary premium (among gold, silver, Bitcion, only Bitoin is pure money without industrial or consumer use). Like Bitcoin, many of the most valuable companies are very large users and/or providers of cloud and high-performance computing and have a strong AI presence. https://companiesmarketcap.com/assets-by-market-cap/

OrionX Constellation™ reports cover 6 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.

Bitcoin’s Dominant Market Cap

> *“What is the value of human freedom?”*
> *– Larry Fink, CEO of BlackRock*

We make two observations about the list in Table 1. It’s mostly a list of American companies that have global footprints. And the companies that dominate the list use huge amounts of computing resources, primarily for AI and cloud services which they locate in multiple data centers. Bitcoin uses huge amounts of computing resources in an even more decentralized manner, to secure the ledger (blockchain) and to mint (or “mine”) additional valuable bitcoins.

Bitcoin now has over 50% of the total cryptocurrency market capitalization. It is worth as much as all other 20,000+ cryptocurrencies combined; perhaps 9,000 of these are still active. The original is worth more than an entire field of imitators. This is not to say all other cryptocurrencies are useless, some will live on, some have produced innovation and find applications.

Stablecoins are useful bridges between fiat currency and the crypto world. They act as a sort of money market vehicle and now can be staked to gather yield. They foreshadow a future with central bank digital currencies. Ethereum has led the way in terms of smart contracts in various implementations (ICOs, NFTs, etc.) and has several viable competitors for those functions.

However, in terms of redefining the technology of money, especially for the store of value attribute, that honor belongs to Bitcoin. We call it Money 3.0 or digital money for our new millennium. It is created and maintained with a security protocol (consensus algorithm) based on Proof of Work, in particular Reusable Proof of Work. Real work and energy input underpin its value.

Currently it is monetary technology with great potential but not yet a clear alternative to the over one hundred fiat monies which rule the planet and are legal tender in every country. Largely that is because it has not grown enough, with a market cap of ‘only’ about 3/4 of a trillion dollars. Yet that market cap is larger than that of all publicly traded companies except for the eight most valuable. Bitcoin is also exceeded in market cap by the two metals with the largest monetary premia, for historical reasons, silver and gold.

You may wonder why Bitcoin has any value at all. Here are two sources: https://www.investopedia.com/ask/answers/100314/why-do-bitcoins-have-value.asp and https://medium.com/the-capital/aristotle-would-prefer-bitcoin-f0f825f87d3f Money should have scarcity, divisibility, durability, portability; these are the Aristotelian attributes. It should also be fungible (one unit is like the next). Bitcoin adheres very well to all of these attributes. Note Aristotle did not mention issuance by the nation-state as one of his four attributes.

The Internet made Alphabet, Amazon, Apple, Microsoft, and NVIDIA huge trillion-dollar companies. Bitcoin is native Internet money or fully digital money that is approaching a trillion dollar market capitalization.

Proof of Work

> *“Proof-of-work has the nice property that it can be relayed through un-trusted middlemen. We don’t have to worry about a chain of custody of communication. It doesn’t matter who tells you a longest chain, the proof-of-work speaks for itself”*
> *– Satoshi Nakamoto [Bitcoin Talk forum, 8/7/2010]*

The Proof of Work (POW) consensus algorithm was first invented by Naor and Dwork in 1993as a method to deter spam and denial of service attacks. Note that we still have to deal with those, because we have not fully deployed proof of work across the Internet. Bitcoin provides a general toll gate and at some point, it may be used much more widely for security purposes. If you want to access a site or send a message, then pay a tiny amount of Bitcoin. This can be done cheaply since it is divisible into 100,000,000 small units, known as Sats, that are currently worth a small fraction of a cent.

Hal Finney invented Reusable Proof of Work (RPOW) in 2004, it allows for reusable tokens and represents the final technological breakthrough that was required to allow for Internet money, fully electronic money. The original proof of work was analogous to putting a single use postage stamp on a message, while the RPOW in Bitcoin's Nakamoto consensus, being reusable, creates permanent 'coins' that can be transferred between Bitcoin addresses. Wallets that have the private keys can transfer Bitcoin from an original address and transaction field within a given block to a new one in a new block, allowing for spending. Hereafter we just refer to it as proof of work, or POW, with reusability implied.

Satoshi solved the double spending problem by requiring a computationally expensive hashing puzzle to be solved such that each block of transactions is added to the timechain (blockchain) by only the single winning system of that block. It then broadcasts the block to the decentralized ledger. The winning system also receives a block subsidy of some number of new Bitcoins (currently 6.25 per 10-minute block, but just half that after April next year). Blocks are stored on thousands of full nodes for which only an inexpensive laptop or Raspberry Pi system is required to hold the entire transaction history of Bitcoin over its 15-year life history.

So, POW as implemented in Bitcoin is a supercomputing problem currently requiring millions of specialized ASIC-based computers located around the world, but especially in the U.S. and a few other countries. Notably the hash rate, that is a measure of how many SHA-256 cryptographic hashes performed per second for the continuous global lottery competition, used to be dominated by China until their ban.

Unwisely, China banned Bitcoin mining in 2021 and the hashrate migrated, especially to the US and to other central Asian countries including Russia and Kazakhstan.

In the supercomputing world we are proud of our highest-end Exascale systems. Well Bitcoin now has in aggregate over 500 Exahashes/second. That is half a Zettahash, (one Zetta is a thousand Exa) we are entering the Zettascale era for Bitcoin supercomputing. These are not floating point calculations, but a single hash is an involved multi-step bit manipulation process that is best calculated using custom ASICs. Most are manufactured by TMSC. The scale of global Bitcoin mining is that it employs several million of these systems at any instant.

> *"Proof of work is not only useful but absolutely essential. Trustless digital money can't work without it. You always need an anchor to the physical realm. Without this anchor a truthful history [ledger] that is self-evident is impossible. Energy is the only anchor we have."*
> *– Gigi, **21 Lessons**. "Proof of work = trust physics…proof of stake = trust humans".*

Bitcoin Energy Usage

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 0.5 Zettahashes/second. And every four years there is a Halving ("halvening" or even "Halfining" 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.

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 next Halving will be in late April 2024, and it will reduce the block subsidy from 6.25 for the winner of the block lottery to 3.125 bitcoins. Bitcoin mining is extremely competitive and only the most efficient miners with access to low-cost electricity and recent generation mining hardware can succeed. The miners have to fight over a shrinking block subsidy amount. Fortunately for them, the price of Bitcoin has moved up strongly over the long term, although with high volatility. And transaction fees are also part of the block reward and will become a larger percentage of the total reward over time.

Currently according to the Cambridge Center for Alternative Finance, the global energy usage is around 15 GigaWatts, or 132 TWh per year. It has approximately doubled over the past four years, since late 2019. But from CY 2021 to CY 2022 it increased just 7%. When the next Halving occurs, the less efficient mining rigs will be shut down unless the price of a bitcoin increases considerably.

Meanwhile the energy efficiency of mining hardware has improved by well over a factor of two in energy efficiency over the last four years. The current average is about 30 Joules per Terahash/s. Typical rigs have over 100 Terahash/s of hash power, the very newest announced are at 200 Tera or more.

Greener than Average, a Circular Asset

The estimated CO2e for global Bitcoin mining is 67 million tons per annum, this is quite sensitive to what fraction of the electricity is derived from coal. Bitcoin miners having been moving toward greener sources, and according to the Bitcoin Mining Council, their membership has 2/3 of its electricity input derived from sustainable sources (including nuclear power). The BMC estimates 60% of global mining is based on sustainable electricity while the CCAF estimate is 62% is based on hydrocarbons. The BMC numbers are more recent, 1H 2023 and the CCAF estimate is for 2022. The BMC numbers are more directly gathered from miner statistics while the CCAF statistics were derived from a survey of a few mining pools (brokers of hash rate).

The shift away from mining in China has been favorable toward Bitcoin increasing its green percentage, because although China had used a lot of hydropower, the out-of-season alternative was mostly coal-based power.

On balance it appears that at least half of Bitcoin mining is based on solar, wind, nuclear, hydropower and geothermal sources and that is better than the world's electricity mix in general, which is 39% green and nuclear at present. It is in Bitcoin miners' economic interest to locate with those sources because they are generally cheaper, and because during times of peak electricity demand, Bitcoin miners can quickly reduce or shut in fully their usage. Often, they receive financial incentives from their electrical utilities to do this.

What commentators who bemoan Bitcoin's energy usage consistently overlook is that Bitcoin is a production process; permanent value is produced. Bitoin is permanently transferable value. Most electricity is used for consumption, to run appliances, lighting etc. And that's useful. But producing one bitcoin with electricity is analogous to mining, refining, and minting the equivalent of 18 one-ounce gold coins, with permanent value that rises in gold terms. All those steps needed with gold are compacted into a single ten-minute digital process. And it is much easier to confirm the legitimacy on the ledger of Bitcoin than it is to assay gold.

Year	Average Market Cap $B	Annual Miner Revenue	% of Market Cap
2016	8.95	0.57	6.4%
2017	65.9	3.37	5.1%
2018	129	5.5	4.3%
2019	132	5.2	3.9%
2020	205	5.01	2.4%
2021	892	16.8	1.9%
2022	535	9.51	1.8%

Table 2. Miner revenue and average market cap by year. Data Source: Glassnode. The aggregate miner revenue since 2016 is $46 billion but the current market cap at $665 billion is 14 times as large. In only 7 years the market cap climbed from $9 billion to the present-day cap of $655 billion (see Table 1).

In Table 2 the average market cap by year since 2016 and the annual miner revenue are summarized. The miner revenue has been steadily falling as a percentage of market cap because it essentially tracks the inflation rate for Bitcoin, the relative amount of new supply. From 2016 the market cap climbed from $9 billion to $535 billion average in 2022. Currently it is $665 billion (Table 1). The miner revenue during that period totals $46 billion, but the economic value has climbed to be 14 times greater. For tens of billions in expenditure on electricity and computing equipment, hundreds of billions of economic value has been ultimately created, as the market cap climbed much faster than the expenditure.

In a word, Bitcoin is highly circular, a persistent circular economy asset. It can be reused an hour after it is created, or a day later, or a week, or a year, or a decade later. And it can be reused repeatedly with low friction. It is highly divisible, with the smallest amount being one Satoshi or Sat, being just 0.00000001 bitcoin, less than 1/3000 of a dollar.

The seigniorage margin is presently much better with Bitcoin than gold, it might cost the miner $125,000 on average in electricity, other operating costs, and in capital equipment amortization costs, to win a block with 6.25 bitcoins worth $225,000 or so, at present prices. Since electricity is roughly half of their input costs, getting access to cheaper electricity makes all the difference.

Top 6 POW Coins

There have been thousands upon thousands of attempts to copy or “improve” upon Bitcoin. Every one of these has failed to exceed Bitcoin in importance and market capitalization. Most of them have abandoned proof of work, by chasing transaction scaling, but sacrificing the security and ensured scarcity and greater decentralization that POW provides. A sound digital money should have security and scarcity to impart long-term value, and for it to be an alternative to existing fiat systems, it should have decentralization, private issuance, and a decentralized shared ledger. Transaction scaling is best handled by a layered architecture, just as the Internet architecture is layered and existing fiat monetary systems are layered with base money (central bank reserves), retail money, and higher layers of transactions and settlement.

Coin	Market Cap (B$)	Total hash rate and Algorithm	Annual Production rate $B (nominal)	Current Supply (millions)	Max Supply (millions)
Bitcoin	665	479 Exa, SHA-256	11.20	19.52	21
Dogecoin	9.69	716 Tera, Scrypt	0.42	141,450	infinite
Litecoin	5.00	784 Tera, Scrypt	0.09	73.77	84
Bitcoin Cash	4.73	2.52 Exa, SHA-256	0.08	19.53	21
Monero	2.97	2.34 Giga, Random X	0.03	18.35	Infinite
Ethereum Classic	2.33	154 Tera, ETCHash	0.10	143.55	210.7

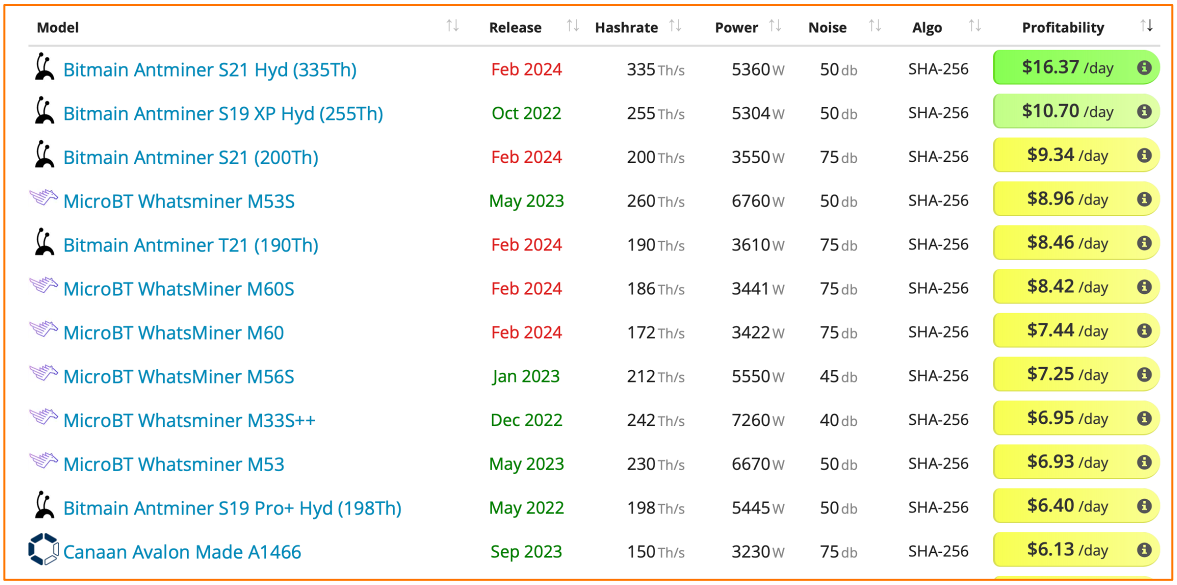
Table 3. Top 6 POW coins as of 10/28/23, data source: miningpoolstats.stream . Only Bitcoin and Dogecoin exceed our cutoff of 0.25 billion dollar annual production rate.

Since this is a CryptoSuper report, we only consider POW coins that have very high computational requirements to secure their ledgers and their value. The top 6 POW coins by market cap are Bitcoin, Dogecoin, Litecoin, Bitcoin Cash, Monero, and Ethereum Classic. Note that the 'original' Ethereum, now called Classic, used POW, this is the original coin. The current better known Ethereum underwent a fork (via committee decision) and roll back of the ledger when it suffered the DAO attack early in its life. And then it moved to Proof of Stake in September 2022.

From Table 3 above one readily sees that the POW coin production is about $12 billion per year, and that Bitcoin completely dominates the production of annual economic value.

Top Mining Rigs

As seen in Table 4 below most of the latest mining rigs currently available produce from 140 to 260 Terahashes/sec. Thus if the global hash rate at present is 500 Exahashes/s, it takes two to three million of these latest mining rigs to produce the global hash rate. Of course, many earlier generation mining rigs at about 100 Terahashes/sec or less are still in production, it's a mix of newer and older equipment. Typical power requirements are 3 kiloWatts to 5 or more KiloWatts for water-cooled "Hyd" as in "hydro" rigs. The most popular brands are Bitmain's Antminer, MicroBT's WhatsMiner, and Canaan's Avalon. These are mostly manufactured in China using ASICs supplied by Taiwan's TSMC, but Samsung is also reportedly manufacturing SHA-256 algorithm ASICs for Bitcoin mining. GPUs are used for some lesser coins but are not competitive with custom ASICs for Bitcoin and Dogecoin mining.



Model	Release	Hashrate	Power	Noise	Algo	Profitability
Bitmain Antminer S21 Hyd (335Th)	Feb 2024	335 Th/s	5360 W	50 db	SHA-256	$16.37 /day
Bitmain Antminer S19 XP Hyd (255Th)	Oct 2022	255 Th/s	5304 W	50 db	SHA-256	$10.70 /day
Bitmain Antminer S21 (200Th)	Feb 2024	200 Th/s	3550 W	75 db	SHA-256	$9.34 /day
MicroBT Whatsminer M53S	May 2023	260 Th/s	6760 W	50 db	SHA-256	$8.96 /day
Bitmain Antminer T21 (190Th)	Feb 2024	190 Th/s	3610 W	75 db	SHA-256	$8.46 /day
MicroBT WhatsMiner M60S	Feb 2024	186 Th/s	3441 W	75 db	SHA-256	$8.42 /day
MicroBT WhatsMiner M60	Feb 2024	172 Th/s	3422 W	75 db	SHA-256	$7.44 /day
MicroBT WhatsMiner M56S	Jan 2023	212 Th/s	5550 W	45 db	SHA-256	$7.25 /day
MicroBT Whatsminer M33S++	Dec 2022	242 Th/s	7260 W	40 db	SHA-256	$6.95 /day
MicroBT Whatsminer M53	May 2023	230 Th/s	6670 W	50 db	SHA-256	$6.93 /day
Bitmain Antminer S19 Pro+ Hyd (198Th)	May 2022	198 Th/s	5445 W	50 db	SHA-256	$6.40 /day
Canaan Avalon Made A1466	Sep 2023	150 Th/s	3230 W	75 db	SHA-256	$6.13 /day

Table 4. Top Bitcoin mining rigs, and estimated probability if electricity cost is 6 cents per kWh, as of 10/28/23. The S21 and T21 models from Bitmain and M60 models from MicroBT will not be available until early next year. Source: https://www.asicminervalue.com/

The gross operating profitability of a Bitcoin mining rig is a few dollars a day, around $10 best case at 6 cents per kWh; mining farms aggregate hundreds and thousands of mining rigs in to racked configurations. Essentially, they are operating Bitcoin supercomputer data centers and search for the lowest cost power and cooling environments with stable regulatory environments.

To give a feel for pricing, the Antminer S21 available early in 2024 has a promotional price of $14 per Terahash or $2800 when ordered in large quantity of 6000 units or more.

Top Public Bitcoin Mining Companies

Collectively, just the 12 publicly traded Bitcoin miners shown in Table 5 have a bit over 100 Exahashes/sec installed, representing over 20% of the typical global hash rate (534 Exahashes/sec on 10/28/23). With this they produce 182 of the new 900 Bitcoin rewarded per day on average. Fees contribute only a few percent in addition to the block subsidy. Not all the installed hash rate is active at all times, for various reasons, including maintenance, upgrading, and curtailment when the Bitcoin price is relatively low or if their utilities ask the mining facilities to shut in due to high customer demand for power.

The 182 coins per day is a 20% share of global production and amounts to some $2.3 billion as an annual production rate. This is an underestimate of what publicly traded miners produce at their facilities. First, we have included only the top 12 companies in this table, and secondly, many of the mining companies host mining rigs for customers under contract, producing additional Bitcoin. All in all, it appears that at least 1/4 of all Bitcoin mining production is from publicly traded miners, and most of that production is in the US and Canada.

The most efficient miners have production costs below $10,000, this does not account for mining rig capital costs of a comparable magnitude, only for operating costs. But with the Bitcoin price now back above $30,000 they can be quite profitable. Their problem is next year the block subsidy will be cut in half from late April 2024, so they need to invest in the newest mining rigs such as the Antminer S21 that aren't even shipping yet.

Company	Market Cap $Million	Locations	Stock Price $	Hash Rate installed by year end Exahashes/sec	Bitcoin Held in Treasury	Daily Bitcoin mined
Riot Blockchain	2,110	US	10.67	12.5	7,327	12.1
Marathon Digital	2,060	US, UAE	9.76	23.1	13,111	32.5
Cipher Mining	780	US	3.14	7.2	518	13.5
Clean Spark	710	US	4.70	9	1,194	21
Hut8 Mining	510	Canada	2.29	2.6	9,366	3.7
Bitdeer Technologies	340	US, Bhutan, Norway	3.10	8.7	0	16.1
Bitfarms	330	Canada, US, Argentina, Paraguay	1.21	6.3	703	13.7
Canaan	320	US, Kazakhstan	1.93	2.0	1,125	3
HIVE Blockchain	290	Canada, Sweden, Iceland	3.41	3.6	2,332	9.2
TeraWulf	280	US	1.25	7.9	N/A	11.0
Core Scientific	260	US	0.70	15.1	1,914	32.1
Iris Energy	230	Canada, US	3.50	5.5	N/A	14
Totals	8,220			103.5	37,590	182

Table 5. A dozen of the largest public companies in the Bitcoin mining space. Although they have collective market cap of over $8 billion. The aggregate market cap for the list is now $1.5 billion higher than in our last report, because of the substantial recovery in Bitcoin price during 2023. The 182 daily Bitcoin mined across these 12 companies represents a 20% share of the nominal 900 Bitcoins generated per day. Collectively the companies hold over $1.2 billion of treasury Bitcoin. Snapshot as of October 25, 2023. Information sources: companiesmarketcap.com and company web sites.

Miners are seeking out renewable and nuclear energy inputs. Increasingly these are lower cost and miners can agree to load shedding under periods of peak electricity demand. In addition to solar, wind, and hydro and nuclear power, capturing methane at the source is very positive for the environment. Methane is from 25 to 80 times worse than CO2 as a global warming contributor. Capturing methane that would be vented from a natural gas field or a landfill is very desirable. Capturing flared methane is also a net positive since flaring is only around 90% efficient at conversion to CO2 and water.

Geographic Distribution of Mining

The Cambridge Centre for Alternative Finance was previously monitoring the geographic distribution of Bitcoin mining. Unfortunately, they have not updated their map and data since January 2022. At that time, they showed the following breakdown: US 38%, China 21%, Kazakhstan 13%, Canada 6%, Russia 5%, others 17%. China had banned Bitcoin mining in Q2, 2021 and this number reflects a drop by a factor of roughly three in their share.

There is probably still substantial hidden mining protected by local authorities and perhaps mining with the approval of the Communist Party, possibly for the government or other favored entities, still proceeding in China.

Kazakhstan’s share has probably dropped because they implemented a stronger licensing regime and a modest tax on the electricity input. Canaan lost half of their overall hash rate due to license suspension in Kazakhstan but have reapplied for a new license.

What does seem to be the case based on the distribution of mining farms owned by publicly traded companies is that between the US and Canada we can account for close to half of all mining. Europe other than Russia has too high energy prices to be a significant player although in northern Scandinavia there are some attractive locations with very low power costs.

Top Pools (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. Their 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.

Mining pools are not miners themselves, although they may own or manage affiliated crypto mining farms.

Pool	Country	Bitcoin AEV ($M)	Dogecoin AEV ($M)	Total $M
Foundry Digital	USA	3,460	0	3,460
AntPool	Global	3,146	48	3194
ViaBTC	USA	1,328	115	1443
F2Pool	Global	1,235	72	1307
Binance	USA	827	0	827
Marapool	N/A	548	0	548
Luxor Tech	USA	245	0	245
BTCdotcom	Global	221	0	221
Braiins	Global	163	0	163
SBI Crypto	Japan	140	0	140
Poolin	USA	105	14	119
UltimusPool	USA	105	0	105
Top 12 operators		11,523	249	11,771
All Mining		11,651	370	12,021

Table 6. The top dozen mining pools and their current rate of winning blocks converted to an annual economic value of Bitcoin production run rate. Several of the pools also mine Dogecoin as well as Bitcoin. The Bitcoin annual economic value also includes 3% of user paid transaction fees, a recent typical value. The top 12 mining pools represent over 98% of the mined value from known hash rate. Bitcoin has a 97% share of the $12 billion annual economic value (AEV).

Five Year Anniversary of Crypto Super Reports

Our first CryptoSuper500 report was five years ago, in November 2018. While there are over 20,000 “cryptocurrencies” that have been created in the interval, only 39 of these coins plus 5 stable coins tied to fiat have valuations above $1 billion. Most projects have been abandoned or are worth little; most were essentially and 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.

At that time the Bitcoin market cap was just over $100 billion, as compared to nearly ¾ of a trillion $ today. In the table below we summarize a few attributes such as market cap and hash rate. These have been roughly doubling every two years.

Attribute	Nov. 2018	Nov. 2023	Compound annual growth rate, past 5 yrs.
Coins making cut for CryptoSuper report	Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Monero	Bitcoin, Dogecoin	Consolidation
Number of different cryptocurrencies	2000	9000 active, over 20,000 total	Majority abandoned, or worthless
Bitcoin Market Capitalization	$111 billion	$665 billion	43%
Bitcoin Price	$6,334	$34,091	40%
Bitcoin annual production $ run rate	$4.2 billion	$11.2 billion	22%
Bitcoin Hash Rate Exahash/s	57	518	56%
Cryptocurrency Market Cap	$220 billion	$1250 billion	42%
Top cryptos annual mining production $	$5.6 billion	$11.6 billion	16%

Table 7. Key attributes of Bitcoin and major cryptocurrencies, comparing the first CryptoSuper report in 2018 with this report 5 years later. Recent data is as of 28 October 2023 except price and market cap are as of 13 November. 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.

Note that the Bitcoin and total cryptocurrency market caps have grown roughly as Moore's law, that is over 40% compounded and thus doubling every two years. The annual economic value of the production of Bitcoin by miners has grown at a more modest 22% rate as the supply was curtailed by the Halving event in April 2020. (The next Halving event, cutting the block subsidy in half once again, is due in April 2024).

The annual mining production of the top cryptos (down from five different coins to only Bitcoin and Dogecoin) has grown at a more modest 16% compound rate. 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 ago.

In 2018 roughly 2/3 of mining hash rate was in China. Due to the Chinese mining ban in May-June 2021 this has dropped to around 1/5. The US has quickly become the leading source of mining hash rate and of all hash rate around 1/5 is due to venture funded startup mining companies with facilities 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 appears to be produced by more than 50% green or nuclear sourced power.

Bitcoin Use Cases

Bitcoin has demonstrated three major use cases at scale. The first is transmission of moderate to large or even very large value amounts across the globe within an hour. Usually, six blocks of 10 minutes' duration are considered adequate for strong confirmation of a transaction. This is much faster than moving money through the international wire system (SWIFT), and the fees are lower.

The second well established use case is that of longer-term savings. While Bitcoin is highly volatile, its long-term price trend has been strongly upward. More recently volatility has decreased toward NASDAQ index levels. It is useful as a savings or reserve store of value for individuals, families, businesses, and corporations, and potentially, governments. In this regard it has often been referred to as a type of 'digital gold', or 'electronic gold' but has grown in value significantly faster than gold has in the past decade.

The third well established use case is freedom from the banking system, "be your own bank". You can save your Bitcoin in your own hardware or software wallet and no one else has access to it. You can also set up multi-key configurations for wallets, for families or companies. It can be like a private safe or a safety deposit box with the custodian sharing key access with the client.

There are several additional use cases that are in their earlier stages. Bitcoin can be used for retail transactions, as a daily medium of exchange. Small purchases using Bitcoin on the base layer are not rapid enough in comparison to cash or mobile payments or credit cards. But the second layer and side chain solutions completely change this. Lightning, a second layer to Bitcoin, has extremely low costs and is very rapid and can thus be used for retail purposes. Its volume is small, but growing quickly, by around a factor of 13 in the past two years. The technology works on the second layer by opening channels between parties that are only settled back to the main Bitcoin time chain (blockchain) in batched transactions at some later date. Conceptually it's not different from you loading money on your Starbucks card that you will not use until three days from now or a week later.

Lighting can even be used as an intermediate payment rail for fiat. In fact, it is already used by the Square app for international transfers from one fiat to another with Lightning under the hood.

Bitcoin may be used for tokenization of assets such as stocks, bonds, and real estate. Several blockchains, typically proof of stake chains, are also being deployed toward this use case. But with the Segwit (segregated witness) and Taproot extensions to the Bitcoin protocol, more flexible smart contracts are now possible. We have even seen a robust NFT market develop on Bitcoin rather than on Ethereum or other POS coins, using an individual Sat inscriptions method that allows for data objects to be stored in the address field of Bitcoin. If you're going to tokenize an asset, why wouldn't you want to do that on the most secure chain available?

In the next section we discuss the use case for governments to consider Bitcoin as a strategic reserve asset. We know that governments are actively looking to digitize their fiat currencies with CBDCs (central bank digital currencies).

CBDCs and the Geopolitical Outlook for Bitcoin

> *"What Satoshi set out to do was completely change the entire power structure on Planet Earth. This is not just a piece of technology, like the iPhone. It's a complete revolution."*
> *– Fred Krueger, Investor*

In the discussion of Bitcoin and CBDCs it is important to remember that money is layered. The base layer is monetary reserves or bankers' money that is not used by the public or non-banking businesses. Above that are the retail layers of cash and checking deposits. There are higher layers such as dollars held overseas and credit card advances.

Jason Lowery in his book (and MIT master's thesis) ***Softwar*** says hash power is a valuable military/intelligence resource. He envisages nations engaged in competitive hash power competition. One reason for this is that national security and critical cyberinfrastructure may be protected by portals that require (usually smallish amounts) of Bitcoin to access as another component layer of the security profile. Attackers and defenders will thus want to accumulate Bitcoin and hashing power. The Pentagon seems interested in the concept; they ordered Major Lowery to pull his book from Amazon.

Lyn Alden ends her book ***Broken Money*** with three chapters on the privacy issues around fiat money and especially with mobile payments and CBDCs. When money was coinage, it was privately held, and hard to surveil. Cash, i.e., physical bills is a bit easier, and now there are strict reporting requirements on transactions of over $10,000 cash in the US and similar or tighter restrictions in many other countries. But most money is now digital checking money and easier to surveil. With CBDCs that will be primarily used from mobile devices it will be easier than ever to monitor even very small transactions. Furthermore, how you spend your CBDCs, or whether those funds have an expiration date could potentially be subject to government control. It would be even easier to fully freeze an account than it is now.

She quotes Steven Feldstein of the Carnegie Endowment for International Peace:

> *"AI surveillance technology is spreading at a faster rate to a wider range of countries than experts have commonly understood. At least 75 out of 176 countries globally are actively using AI technologies for surveillance performance. This includes smart city/safe city platforms (56 countries) facial recognition systems (64 countries), and smart policing (52 countries). China is a major drier of AI surveillance worldwide. ..Huawei alone is responsible for providing AI surveillance technology to at least 50 countries worldwide."*
> *– Steven Feldstein*

Military grade spyware tools, including on financial transactions, may keep populations safe, or them may be used to oppress dissidents and human rights advocates.

Matthew Pines sees a reserve asset possibility for the West as a counter to China's Yuan based CBDC and Belt and Road trade route architecture that wants to replace the US dollar with Yuan. We agree in general with his views and believe that China made a large strategic mistake in banning Bitcoin mining. Bitcoin is about individual freedom and runs counter to the ethos of the Chinese Communist Party's collectivist ideology.

CBDCs, digital currencies managed by central banks through the existing banking system, are coming. There has been more and more exploration of the topic by all the major central banks. China, among major countries, was first out of the chute with their digital Yuan or e-Yuan. China's five largest cities now offer the e-Yuan as a payment option. Some government services can be paid for in e-Yuan, and at least two of the large mobile payment providers support it, but usage remains modest.

In Europe, it seems like the intent is strong by the European Central Bank to proceed with a CBDC. They recently completed their investigation phase for an e-Euro, and their preparation phase started November 1, 2023 and will last two years or longer.

> *"We need to prepare our currency for the future. We envisage a digital euro as a digital form of cash that can be used for all digital payments, free of charge, and that meets the highest privacy standards. It would coexist alongside physical cash, which will always be available, leaving no one behind." - Christine Lagarde, President, European Central Bank*

In the US there has been backlash against the CBDC concept because of privacy concerns, and bills have been introduced into Congress opposing CBDC issuance. The Federal Reserve has studied CBDCs, most notably in a project with the Boston bank and MIT but has no plans in place. Their latest focus has been to roll out a faster settlement system between banks, FedNow.

I note that to begin to be a significant reserve asset you only need to rival gold holdings, and for the US that is around 8000 tons at $60 million per ton currently or about $1/2 trillion, and which is something like 4% of all gold in the world. That is less than Bitcoin's current market cap. By comparison the base money of the Federal Reserve system is $5.56 trillion, that is the tip of the inverted pyramid on which the entire $27 trillion US economy and much of the world economy indirectly rests.

Now the US Treasury (or the Federal Reserve) would have to procure over time some $1/2 trillion of Bitcoin or more. This could be done by issuing bonds, and although the money supply would increase, on average it would become harder money if the (special issue) bond proceeds were only used toward Bitcoin purchases. In other words, if over time Bitcoin rose to $12 trillion market cap and the US Government procured 4% of that, it would become $1/2 trillion worth as the price was rising during the interval. And the hard assets backing the US dollar would double.

Two small nations have declared Bitcoin as legal tender alongside their fiat currency: El Salvador, which uses the US dollar, and the Central African Republic which uses a Central African Franc that is largely managed by their former colonial masters, France.

The irony here is that Bitcoin doesn't yet have enough market cap to be interesting to large nation states, but it is interesting to smaller ones already, and as the market cap becomes larger, it becomes more interesting to medium-sized nations. And when and if they start to accumulate, they will drive up the price considerably and might well engender a competition between global central banks and treasuries, just to protect themselves, even though they are wedded to fiat and to the mechanism of CBDCs if they feel a digital currency is required.

It is quite possible we could see a world with CBDCs developing to be the major retail form of money. This has to be managed carefully to avoid deposit disintermediation from commercial banks, destabilizing them. Generally, CBDCs will be hierarchical as the current fiat system is today and issued through the commercial banks, which then may choose to offer interest-bearing options as well. But in that world, it is also possible that the base money, or reserve money, that today is simply bookkeeping entries that offset Treasury bonds, could evolve to include Bitcoin as an underlying asset.

We are a long way from de-dollarization, for many reasons. These include the role of the dollar in trade, the unparalleled ability of the US Navy to patrol global sea lanes, the depth of the US Treasury market, the open capital account of the US, and the dominance of the dollar in foreign reserves (59%, while Euro is 20% and Chinese Yuan only 3%). China is not able to replace the US in any one of these several ways anytime soon. But they and other nations are interested in a world that would have a more multipolar power structure for money.

We have already a somewhat neutral asset, the SDR or special drawing rights of the International Monetary Fund, tied to a basket of major currencies. But these are issued only infrequently, are used only between the IMF and governments, and do not amount to much more than Bitcoin's market cap. And SDRs are just another form of debt, like fiat currencies. Bitcoin does have the two advantages that gold historically presented, of being entirely neutral, and being an asset.

One of the interesting aspects is Bitcoin's implementation as a disinflationary currency (less than 1.7% supply increase per annum this year, only 0.83% next year, 0.40% in 2028 and ever decreasing) and this may be more natural in a world of slowing population growth, high debt burdens, and slowing growth in energy usage. It certainly plays into the electrification and greening of energy in the global economy.

Whether Bitcoin will come to play a role in national currencies and their foreign exchange reserve holdings remains to be seen and will require a significantly large market capitalization for Bitcoin that could happen because of major financial crises. It offers the opportunity for a revolution in terms of privacy, and as a global non-governmental currency.

> *"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***

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 minters 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/backgrounder/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.