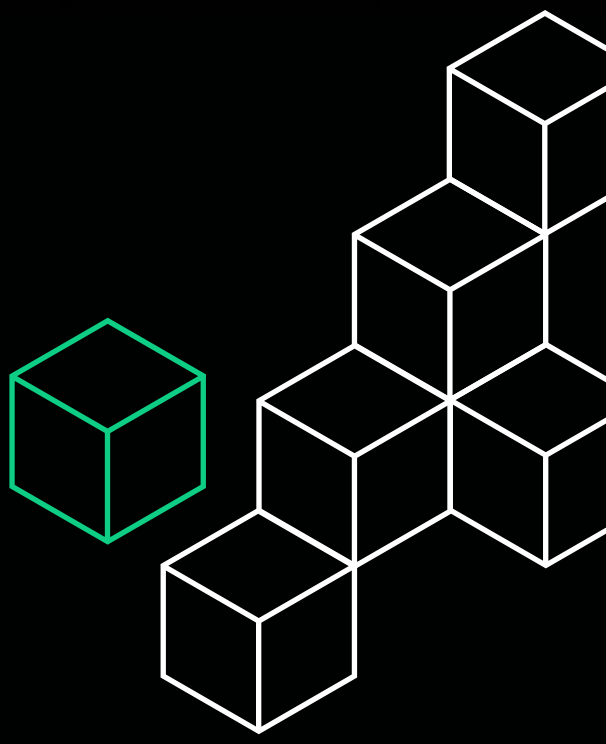
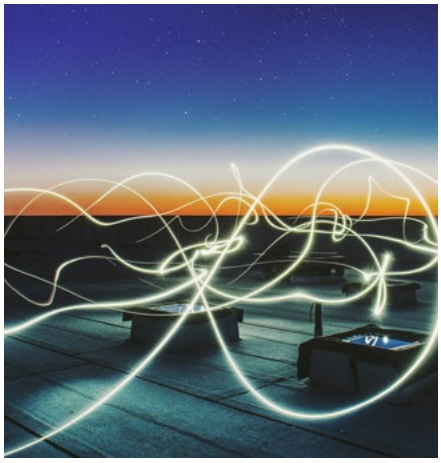
DIGITALWILDCATTERS

CRYPTOEQ

Bitcoin Mining:

A Global Economic Perspective





Crypto is complex.
We make it simple.

CRYPTOEQ

Welcome to CORE+ Reports

At CryptoEQ, we decrease the learning curve to make crypto and blockchain simple. Our CORE+ Reports are the latest iteration that help newcomers and established crypto enthusiasts get a fresh take on the latest trends in the market.

With articles and exhibitions that focus on newest topics, CORE+ will help distill the different ways that blockchain can change the way we think about everything from finance, sporting events, supply chain optimization, and even gaming. You've probably heard of NFTs in the news recently, but even less monetized outlets have seen rapid innovation from enabling and integrating blockchain technology.

As we delve into these complex and multi-modal topics, we hope you will gain a better understanding of the potential that blockchain has to truly transform technology—and the world around us—as we know it.

Contents

Understanding Bitcoin Mining

Executive Summary

Bitcoin “mining” is the process of performing a computational effort to create the next valid block of transactions on the blockchain; a valid block being confirmed across the network sees the creator (miner) rewarded with newly issued BTC. However, taking a step back to understand blockchains, blocks, and transactions is helpful.

Blockchain is a distributed database that tracks the balances of Bitcoin users. Each "block" contains a transaction collection representing the transfer of bitcoins between users, with each transaction represented by an address. Network users broadcast these transactions to a shared network resource known as the mempool (memory pool). The network does not recognize transactions until they have been added from the mempool to the blockchain. To send bitcoins to an address, the sender must include transaction fees to incentivize miners to select their transactions from the mempool. Blocks have a maximum size; therefore, miners (typically) choose to include the transactions with the highest fees, generating maximum revenue for the miner. They then generate a block from these transactions and transmit it across the network so that the nodes may validate it.

Miners

Miners are critical to the network's health, and the idea of including proof of work (PoW) as part of the consensus mechanism (i.e., a network’s process for agreeing on the order of valid transactions) represents a key innovation of the Bitcoin network. Bitcoin miners are responsible for block generation and committing blocks of confirmed transactions to the blockchain. Beyond that, mining aids in:

- Securing the network and preventing corruption from malicious actors
- Minting new bitcoin into circulation in a predictable, predetermined manner
- Maintaining a historical record so that the chain remains auditable and transparent allowing global consensus to be reached

Miners are the global network of computers that:

- Group bitcoin transactions into blocks (since the block size is ~1 MB, each block can only fit so many transactions; should the mempool contain more transactions than can be fit into one block, the transaction overflow will be added to the next block)
- Perform computations to solve a cryptographic puzzle (performing the “proof of work”)
- Bitcoin miners pool ‘valid’ transactions into blocks; anyone can run a Bitcoin full-node and act as a ‘validator’ for proposed blocks; these people are typically miners since they have the incentive to invest in the network’s security
- Send the blocks out over the network to be cross-checked and verified, and they will validate other proposed blocks
- Propagate approved blocks across the network and move on to the next block of transactions

Miners are the backbone of the Bitcoin network and are invested in the network in a way in which investment funds and Hodlers aren't necessarily. As Bitcoin mining hardware has become highly specialized, and economies of scale have facilitated the advent of industrial Bitcoin mining in warehouses, professional miners have emerged, making major capital investments over long time horizons. This investment has led the Bitcoin mining industry to become a global, highly-competitive business.

ASIC Mining Rigs have 4+ year life cycles and can only be used to mine SHA-256 Protocols (almost entirely Bitcoin). Bitcoin mining facilities operate similarly and are typically restructured warehouses specially designed for cooling mining rigs. On average, it will take a miner 18 months to break even after deploying capital to mining rigs, facility buildout, and electricity expenses. To break even and realize a profit, miners must sell the BTC they mine, providing constant sell pressure on the bitcoin price. This sell pressure is especially acute in bear markets and times of distress. The mining industry is living through one of these periods as we speak.

Bitcoin: Miner Net Position Change

 Source

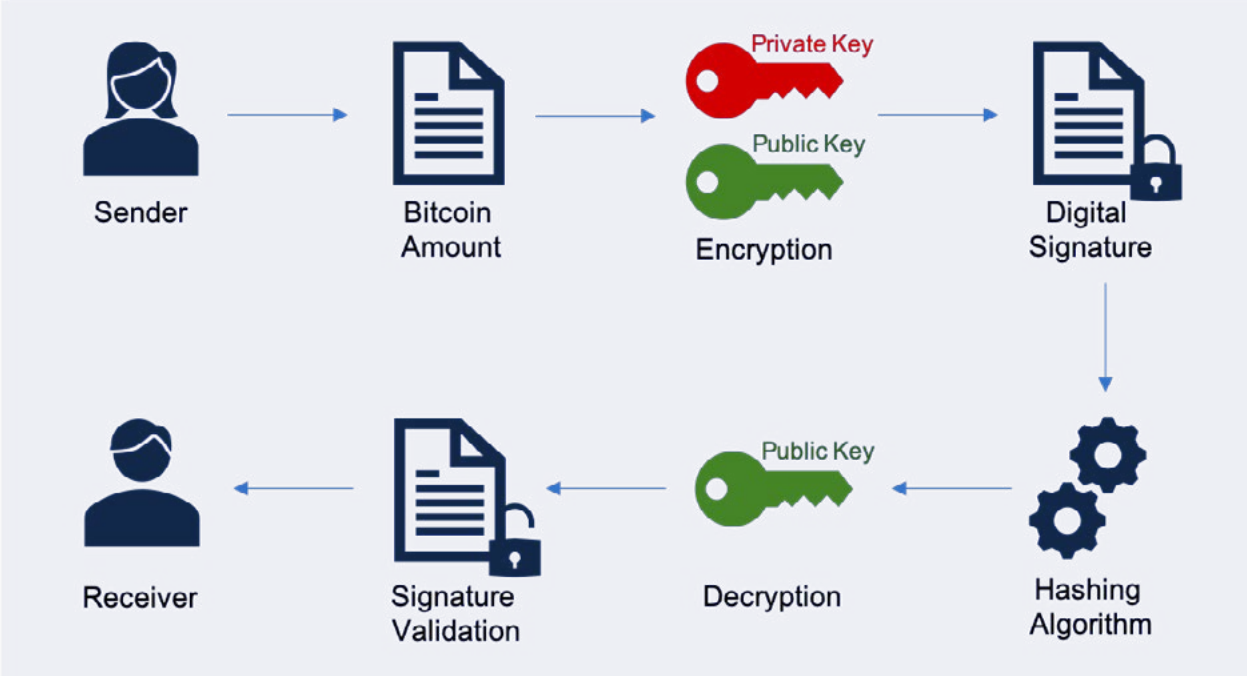
glassnode

On average, it will take a miner 18 months to break even after deploying capital, facility buildout, and electricity expenses.

Proof of Work

Why is Mining Necessary?

Mining is vital to the network security of Bitcoin. To eliminate the requirement for a trusted third party, Bitcoin must prohibit funds from being spent by an unauthorized user or an authorized user multiple times. Digital signatures, a 1970s cryptographic breakthrough, resolve the first problem. The pair of private and public keys offers a strong proof of control that allows only the owner of a private key to spend or transfer bitcoins.



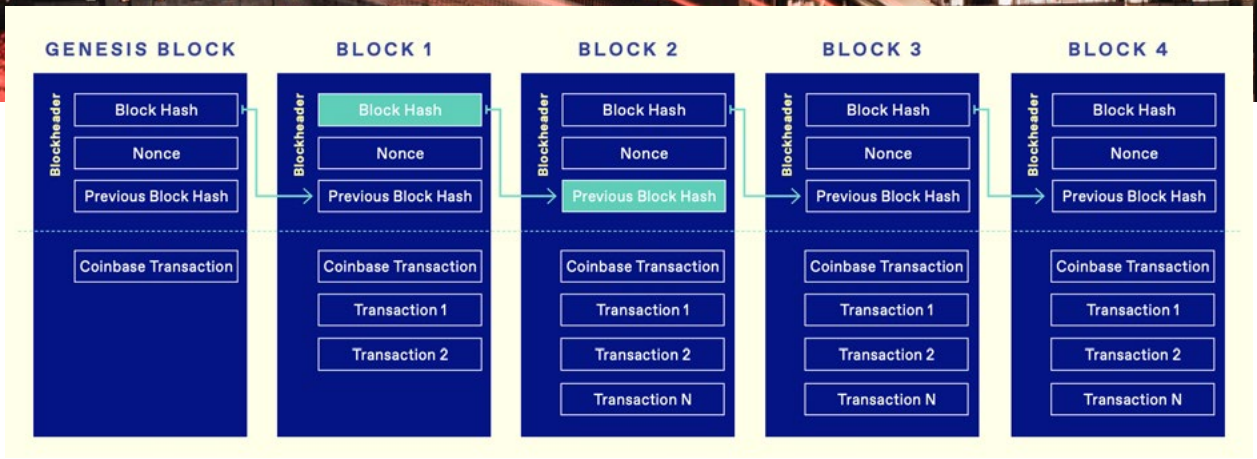
Source

However, digital signatures alone are insufficient to guarantee the recipients of a transaction that the bitcoins they have received have not been sent elsewhere. To provide this assurance, the network must devise a way to validate that the same person cannot spend the same BTC twice. This issue, known as the "double-spend problem," is resolved via PoW based on hash functions, initially conceived by Adam Back in 1997 to prevent email spam. Hash functions are discussed more in the following sections.

PoW enables transactions to be sorted into blocks and added to the chronological chain of blocks dating back to Bitcoin's genesis block. Should conflicting transactions/blocks arise, the network of nodes reaches a consensus on the correct state by examining the chain with the most cumulative hashing power ("heaviest chain rule," discussed more in later sections). Because each new block contains a hash of all the older blocks that have existed, transactions are only reversible if a malevolent actor recomputes all previous PoW back to their attack point, as we will discuss later. Due to the network's continual production of new blocks, it is incredibly difficult for any actor ever to catch up.

Interactive Links

Text that appears **underlined in green** is your entry into an interactive experience! These hyperlinks will bring you to additional sources continuing your educational journey. Please use these to guide your research process.

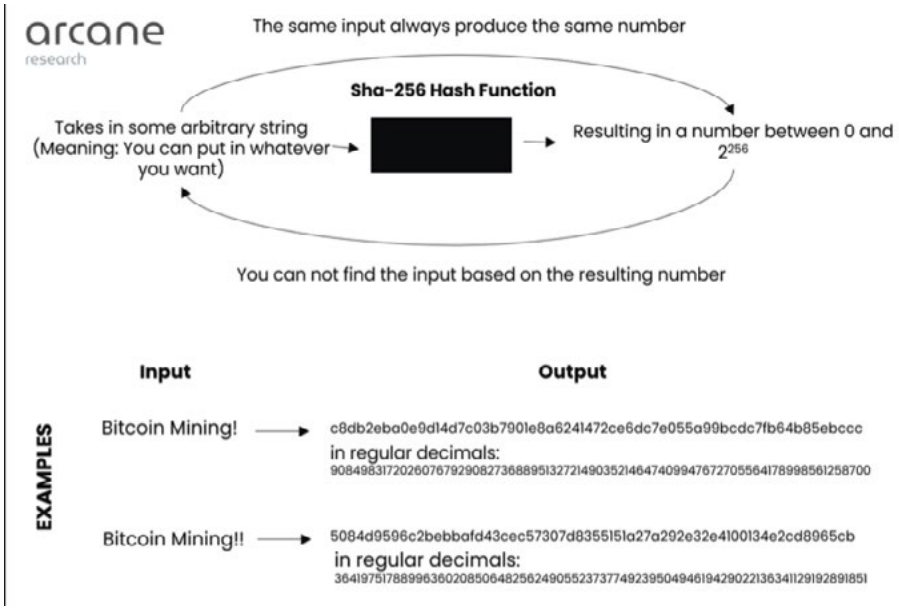


Source: NYDIG Research

The Actual "Work" in PoW

Hash algorithms play a critical part in all cryptography, as well as in Bitcoin. Hashing any amount of data results in a fixed-length hash. Bitcoin and its PoW use the Secure Hash Algorithm, SHA-256, a mathematical function that takes an input of any size and produces a fixed-length output every time. Hash functions are critical private-public key cryptography and have several key characteristics:

- The input into a hash function cannot (realistically) be determined from the output, i.e., it is a one-way function
- The same input into a hash function will ***always*** generate the same output
- The input can be any length, while the output is always the same length. Like all computer data, hashes are large numbers and are usually written as hexadecimal.
- ***Any*** change to the input, no matter how trivial or minute, will change the output
- The output cannot be predicted. It must be guessed—or brute force calculated—by trial and error.



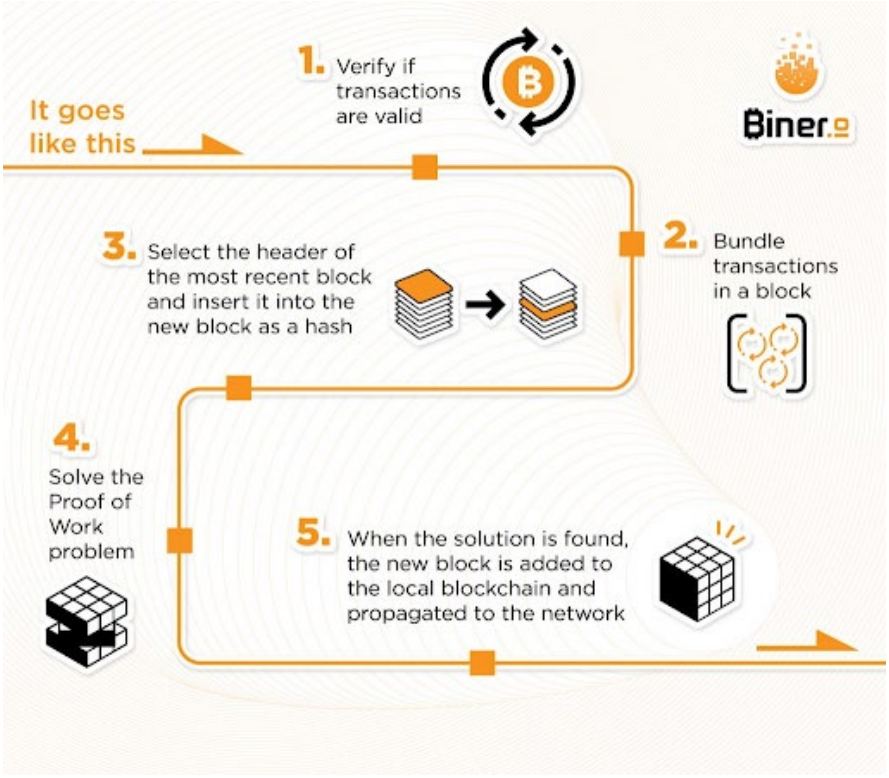
In the PoW Sybil-resistant scheme, Bitcoin miners must try and solve incredibly complex cryptographic puzzles. The mathematical problems can only be solved by “guess and test,” meaning there is no way to gain an edge over the competition other than increasing the number of guesses per second your computer/mining farm can facilitate. Every hash has the same probability of delivering the correct solution making the entire process similar to a lottery.

To properly “solve” the puzzle and create a new block, a miner takes a set of pending transactions from the mempool and runs the data through a hashing function along with a number called a nonce. The "nonce" is simply a random value that miners adjust after each failed attempt. The goal is to discover the correct combination of transaction hash + nonce that is less than or equal to the current target of the network.

If the hash function's output is less than the target, a valid block is discovered, and the miner broadcasts it to the rest of the network. If not, the miner modifies the nonce and runs the identical data through the hash function again.

There are several crucial takeaways from this procedure. First, because this is a high-speed guessing game involving random numbers, the probability that a miner will discover a legitimate block is proportional to its share of the network's hash rate. In Bitcoin mining, size matters, which is one of the reasons mining entities join so-called mining pools, which allow groups of miners to split the rewards of the lucky miner.

The winning miner with the correct nonce adds a new block of verified transactions to the blockchain. If there are more pending transactions than can fit into one block, the unconfirmed transactions wait in the Bitcoin mempool. After confirmation, the transactions form part of a block.



Source

Once miners have solved the puzzle and found the correct answer, they will send their work across the network to be checked by other miners. After all, the entire network must come to a consensus about whether or not this block (and the transactions inside) are indeed valid.

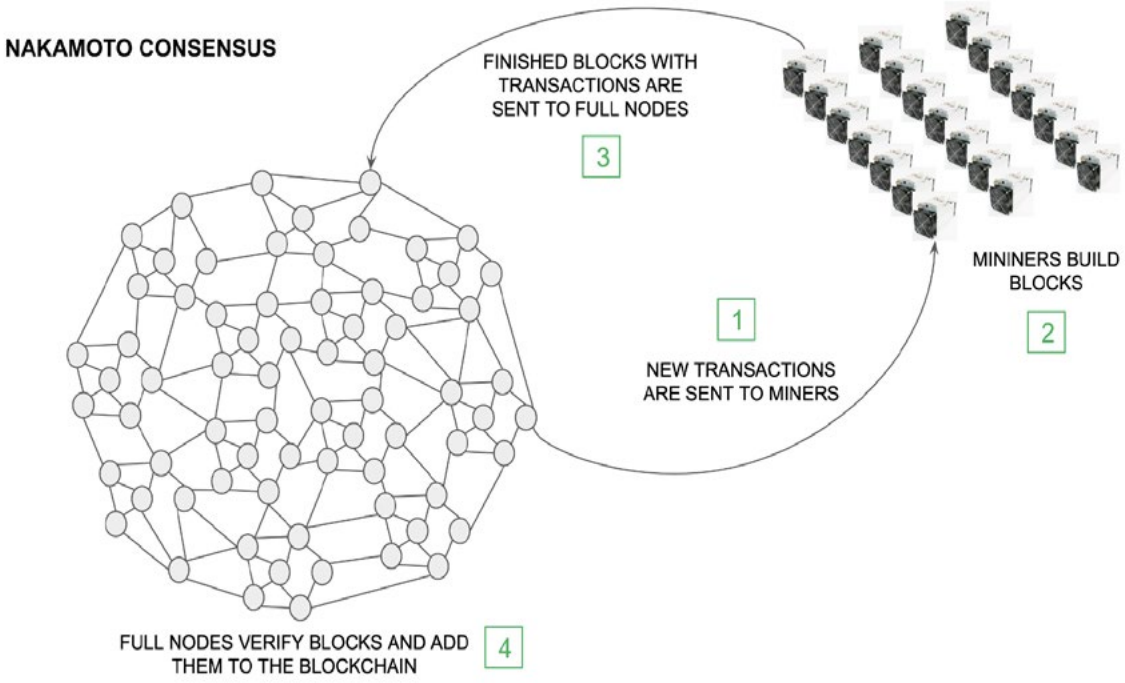
Consensus and Sybil Resistant Mechanisms

Consensus Algorithms

For a decentralized network of nodes/computers to function properly, the independent participants in the network need to agree on a shared state (e.g., who owns what on a blockchain). And while doing this, the network should remain fault tolerant with valid consensus despite imperfect information or malicious actors (Byzantine Fault Tolerance). Different blockchains implement different methods of doing so, but all are attempting to create a "consensus algorithm" that best fits their chain.

Consensus algorithms are used in public blockchain/distributed computer design in order to convince nodes in a decentralized system to agree on the next valid state. Bitcoin uses the established rule that the longest/heaviest chain wins, i.e., the chain with the most computational work behind it. This rule ensures that the proposed block has the required work performed. The longest chain not only determines the sequence of blocks, but also demonstrates that it was formed by the largest computing resource. Therefore, as long as the majority of hashing power is under the hands of honest nodes, they will continue to produce the longest chain and eventually overtake potential attackers.

This protocol, referred to as the "Nakamoto Consensus," creates a system by which a permissionless network can agree on ordering valid transactions while preserving Byzantine Fault Tolerance (BFT). As long as a majority of CPU power is controlled by honest nodes not cooperating to attack the network, they'll generate the longest chain/most work and prevent attackers on the network. PoW makes the Bitcoin blockchain a single, linear version of "truth" that users can trust will not be reversed while also issuing new bitcoins into the network in an unbiased and incorruptible manner.



Source

Bitcoin's Nakamoto Consensus, coupled with PoW, is 100% permissionless and scalable but takes ~30 minutes to one hour for a block to be considered final (relatively high latency). This is because Nakamoto Consensus is probabilistic rather than deterministic. It requires waiting for "enough" blocks to be mined on top of that block so that reorganizing or reverting the blockchain becomes economically impractical, ensuring some "economic certainty" but never theoretic/deterministic certainty.

As a result, Nakamoto chains have high uptime (they do not go down or stall) but low transaction speed due to their probabilistic finalization guarantee. Other proof-of-stake (PoS) networks that use Classical Consensus offer faster finality but do so by limiting the validator set. They do this because, in Classical protocols, validators perform all-to-all communication, requiring more coordination and an updated view of the global validator set. Many PoS consensus algorithms prioritize safety over liveness, meaning the network will halt if issues arise rather than pushing forward anything invalid. This protocol is the opposite of the Nakamoto Consensus.

Would-be attackers in a PoW system who act maliciously have their blocks rejected (because they disagree with the current shared global consensus) and lose out on the bitcoin reward. Not only that, but they also bear the cost associated with PoW mining, thus incurring the cost of electricity without compensation.

Sybil Resistance

One issue with allowing anyone to participate in the consensus of an open network is that one malicious actor can create endless nodes, thereby creating multiple identities, as seen by the blockchain. If one person could create enough nodes, they could theoretically control the network, known as a Sybil attack. For this reason, blockchains also need a Sybil Resistance mechanism in addition to its Consensus algorithm.

On the other hand, a Sybil resistance mechanism is the process through which a decentralized system deters Sybil attacks. A Sybil assault occurs when a single node can flood the network with several identities and utilize them to obtain excessive power.

Ideally, each node in a decentralized system would represent one vote. If a node can impersonate multiple other nodes and get 100, 1,000, or more than 10,000 votes instead of one, then the system is vulnerable to assault. Sybil attacks are often deterred by requiring nodes to show proof of a difficult-to-fake resource (unlike online identities, which are easy to forge).

Proof of Work - Hash power (e.g., Bitcoin)

Proof of Stake - Tokens (e.g., Cosmos, Polkadot, Tezos)

Proof of Space-Time - disk space (e.g., Chia, Filecoin, etc.)

Proof of Authority - (e.g., Algorand)

Block Rewards vs. Fees

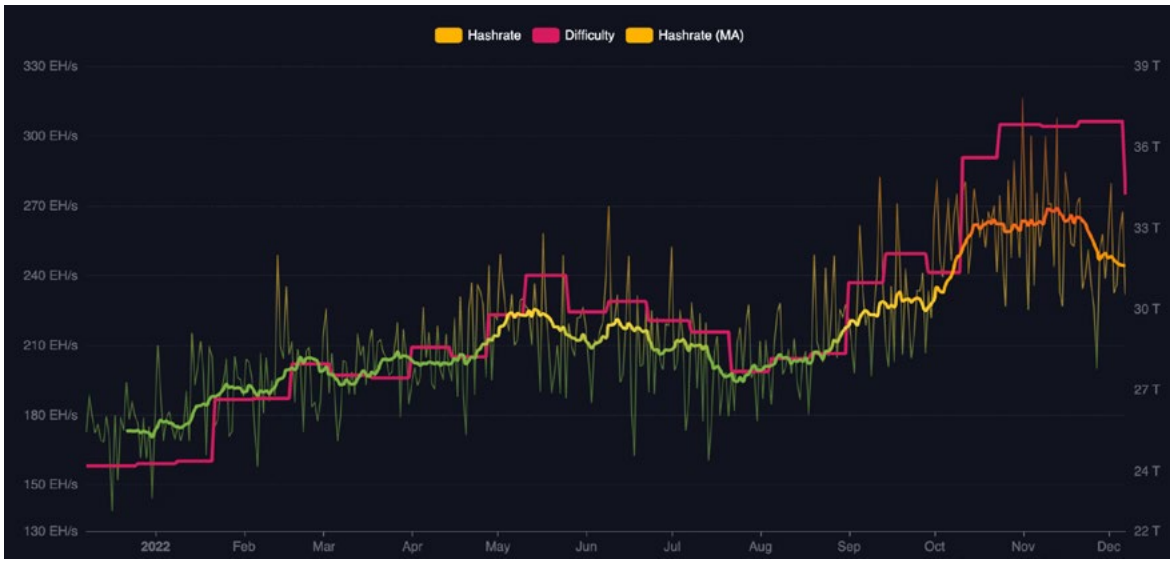
Block Rewards and Difficulty Adjustment

The PoW model engrains real-world costs to the Bitcoin network, making spamming, attacking, or changing the network costly. The economic cost attached to the blocks (electricity, mining rigs, infrastructure, etc.) incentivizes miners to act honestly or else all their work and costs are for naught.

So, why would miners run these vast, expensive computer farms just to solve a quirky puzzle? It's because they get paid in bitcoin for every puzzle they solve that leads to adding the latest block to the blockchain. This reward is called a block reward and is how bitcoins are born.

Despite Bitcoin's popularity and the number of total miners on the network over the years varying greatly, the Bitcoin protocol is programmed to deal with this volatility.

Approximately every ten minutes, a new block is mined, and new bitcoins are created. This consistency and predictability in the monetary policy is part of the magic of Bitcoin. The Bitcoin system was designed to become progressively more difficult to "mine" bitcoins as more computing power is added to the network. This design is known as the Difficulty Adjustment and is a global 'difficulty' parameter that adjusts once every 2,016 blocks (~2 weeks) based on the overall computational power of the network. The difficulty adjustment ensures that the production of blocks and, consequently, the supply of bitcoins remains constant as the network hash rate increases. It does not matter if 100 computers are mining or 100,000,000; the Bitcoin network will dynamically correct itself thanks to the Difficulty Adjustment so that, on average, a new block is produced every ten minutes.

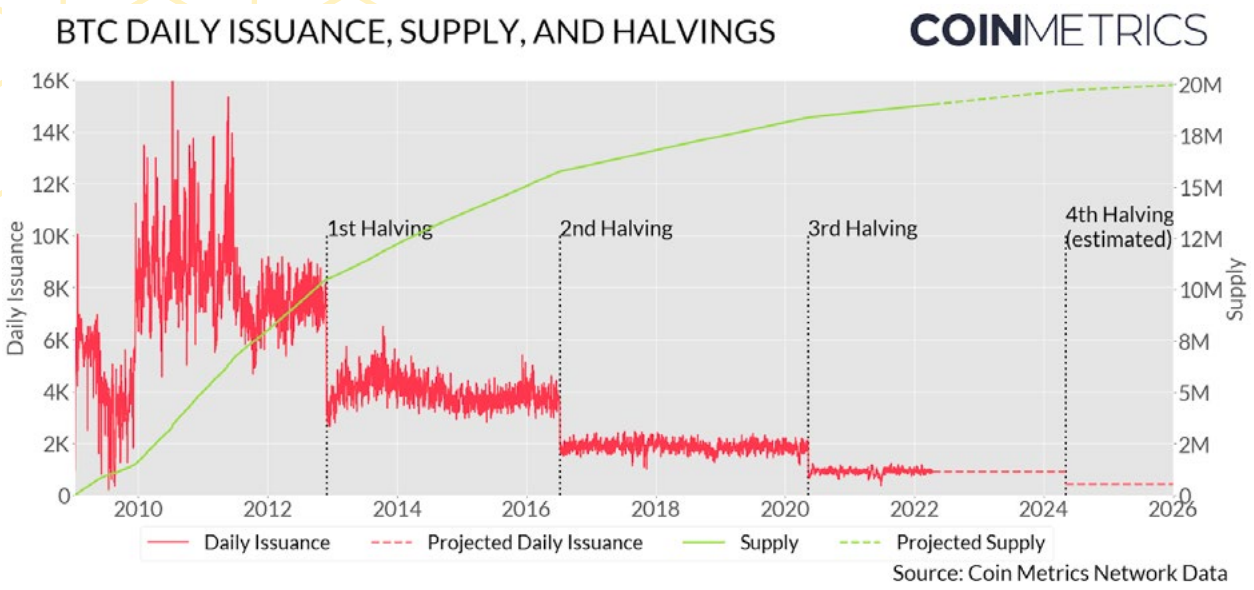


Source

In the long run, there will never be more than 21,000,000 BTC. No matter how high the price of Bitcoin goes, the protocol cannot increase production. Instead, the difficulty simply adjusts higher.

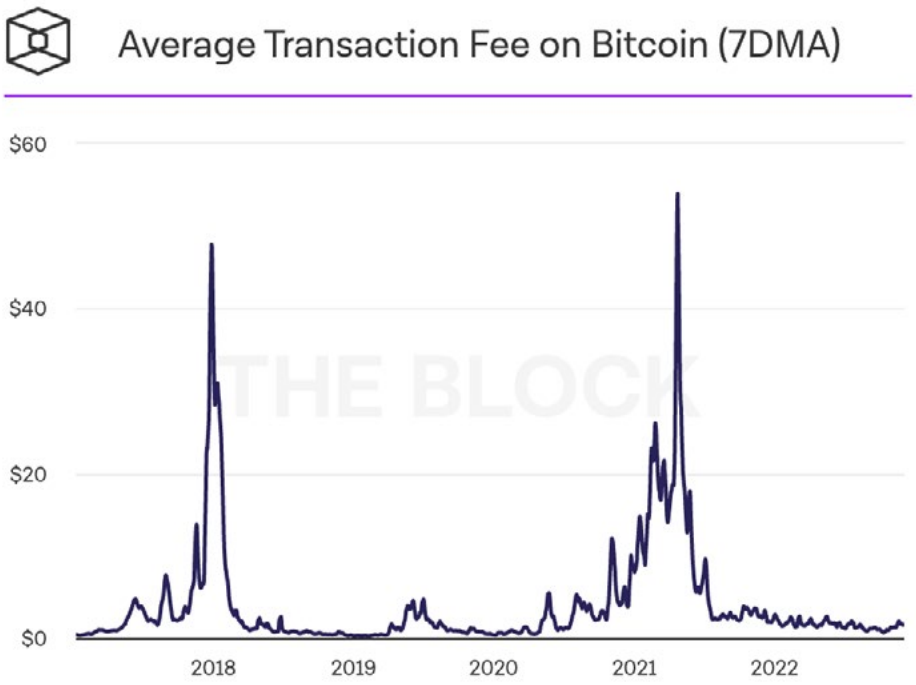
This characteristic makes Bitcoin "mining" very different from the traditional mining of natural resources, where economic drivers—like market price or improved extraction methods—can alter production. For every other commodity or resource, production increases as price increases to capture new profit potential and bring supply and demand into equilibrium. Changes in the total hash rate are accounted for every two weeks by the Bitcoin protocol.

This adaptive structure of the network allows for a very predictable supply schedule, including predetermined "halvenings." In May 2020, Bitcoin underwent its third halvening in which the issuance rate of new bitcoins got reduced by 50% (halved). These halvenings will continue approximately every four years until all 21 million bitcoin have been created sometime around 2140. After that, the miners will no longer receive new bitcoin for their efforts. Instead, they will be forced to sustain their operations through transaction fees for their work.



Transaction Fees

Because miners are profit-driven, they are incentivized to select the transactions with the largest transaction fee, which gets paid to them if they are successful in mining the next block. In times of high demand/network congestion, bitcoin users can manually increase the transaction fees they are willing to pay to increase the likelihood of being included in the next block. This is known as a first-price auction or pay-as-bid mechanism. When the spender's transaction makes it into a block, the miner collects the included fee as a reward. This highest-bidder system enables high-time preference Bitcoin users to outbid low-time preference spenders, ensuring that the most economically critical transactions get confirmed first. Bitcoin transaction fees are highly cyclical, spiking to notoriously high levels ($50+) during bull runs but falling to near-insignificant levels in bear markets (image below).



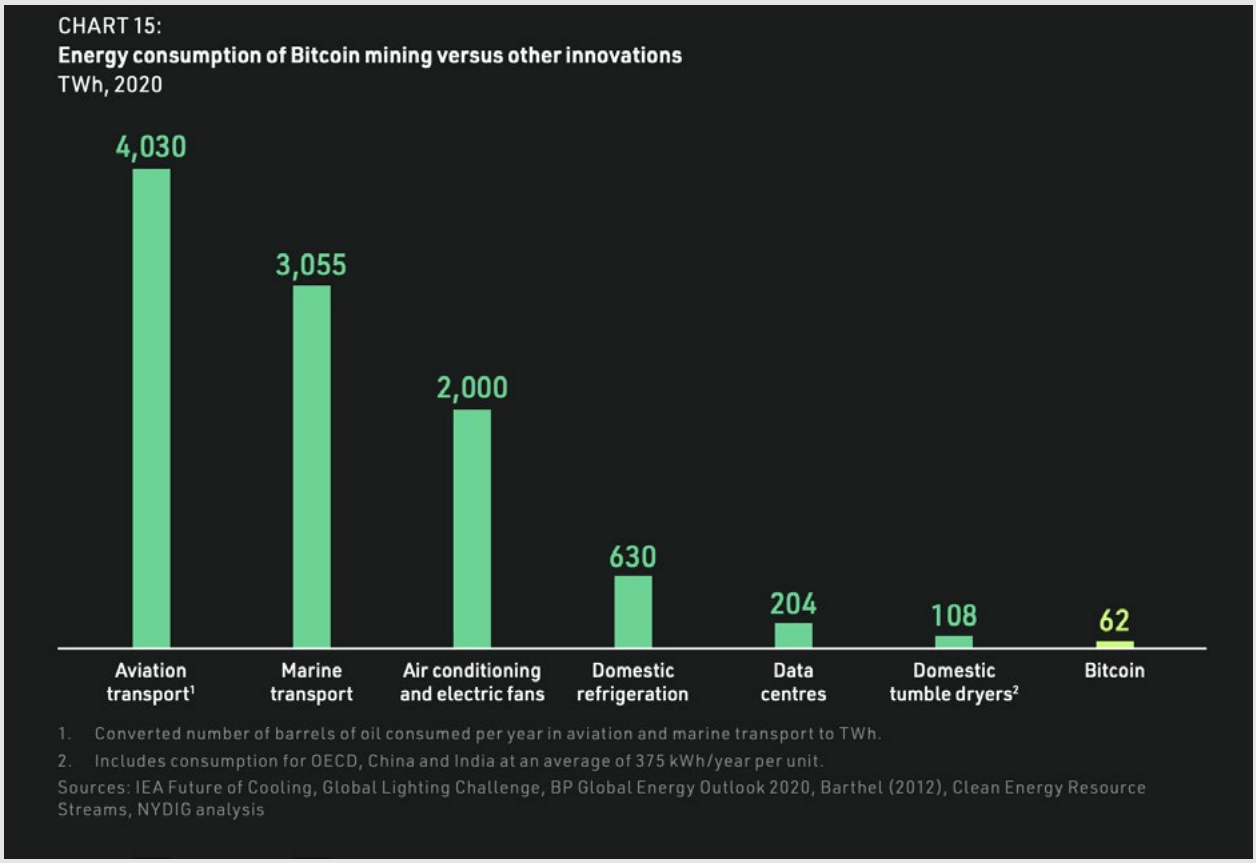
Source

Bitcoin's Energy Use

Context Matters

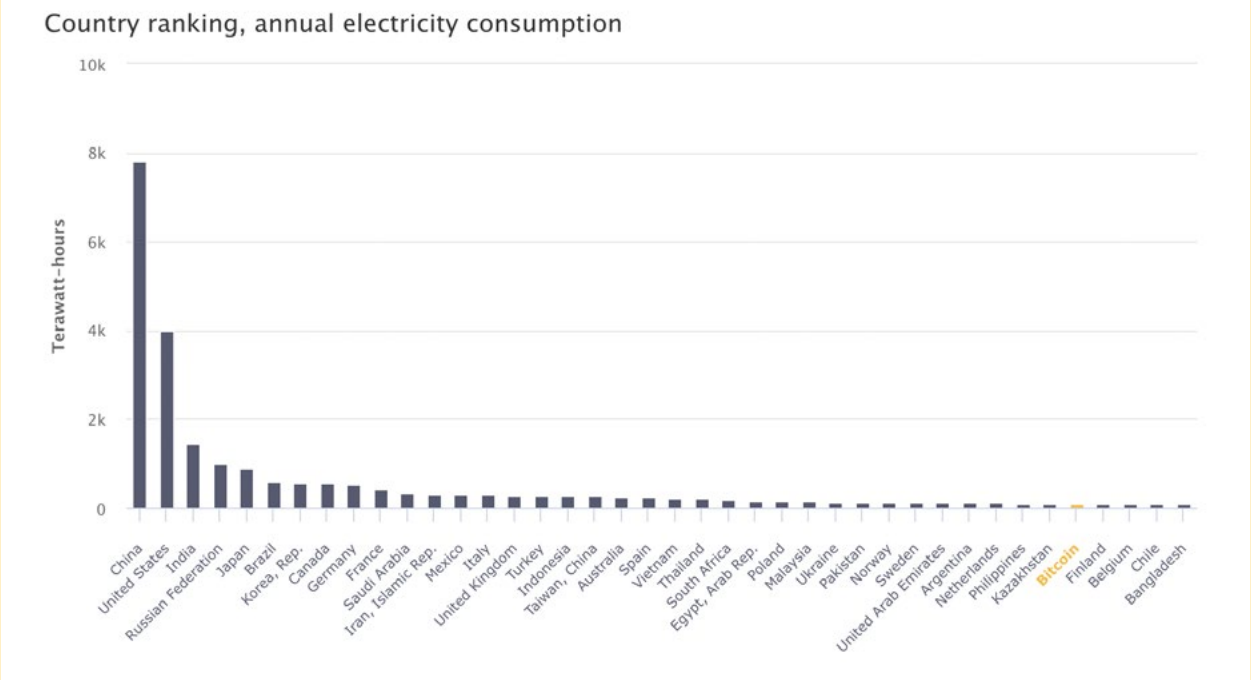
Inarguably, Bitcoin mining utilizes electricity to power its PoW mechanism. Whether it is a lot or a little depends on your frame of reference. But remember, PoW is ***essential*** to a decentralized consensus, network security, and the issuance of new BTC (i.e., Bitcoin's predictable monetary policy). Bitcoin is **not** Bitcoin without PoW.

In absolute terms, Bitcoin mining used an estimated 82 TWh of electricity in 2021, a 9% increase from 2020, according to CoinShares' 2022 report on the Bitcoin mining network. As of December 2021, the current annualized draw is 89 TWh. To put this in perspective, the Bitcoin network consumed 0.05% of the ***total global electricity*** consumed in 2019, essentially a rounding error when it comes to global energy consumption. For comparison, NYDIG reported in Q3 2021 that domestic tumble dryers and data centers used 108 TWh (0.07%) and 204 TWh (0.13%), respectively, in 2020.



Bitcoin energy use versus similar products. Source: CoinShares

Therefore, yes, Bitcoin consumes approximately the same amount of energy as a small nation-state, such as Finland with its ~5 million inhabitants…. Or clothes dryers. Both are true. But strangely, there aren't many (any?) campaigns targeting clothes dryers, data centers, cruise lines, video games, gold mining, etc. In fact, when Bitcoin's electricity consumption is plotted against major polluting countries, the popular argument appears tenuous.



Source

As for 2022, the Bitcoin network is projected to consume an estimated ~114 TWh/yr in total. Meanwhile, the global annual electricity generation is ~27,000 TWh/yr or 237x that of the Bitcoin network. Of that, ~27,000 TWH/yr, the amount of electricity lost in transmission each year is ~2,200 TWh/yr or 19x that of the Bitcoin network (based on World Bank and IEA estimates).

Observing Bitcoin's energy consumption to be similar to that of a small nation makes sense when one sees the utility Bitcoin offers. Bitcoin is a programmable, permissionless, sound currency, something that many nations are not able to provide to their citizens. It is a top-10 base money in the world today. In contrast, the Finnish markka is not one of the top 30, nor used by anyone outside of the 5 million people in Finland.

Despite these eye-opening statistics and comparisons, Bitcoin critics remain unconvinced because they do not see the utility of Bitcoin. However, just because one person doesn't benefit from something, does it give that person the right to try and take it away from those who do? What if this same stance was taken with the above examples? Many people do not play video games or go on cruises. Should they, therefore, cease to exist, too? The fact that these industries exist at all proves that someone somewhere values them. So, why is Bitcoin any different?

Bitcoin's Utility

Bitcoin mining is frequently denigrated for its "wasteful" energy use, which implies that the Bitcoin network is not useful, a claim that Bitcoin's 100's of millions of users might refute. The energy, and associated costs, required to secure the network are precisely how Bitcoin generates its security. If there were no costs, then there would be no security.

The Bitcoin network's energy efficiency and utility are not comprehensively understood by focusing entirely on the particulars of mining; broadly, it is essential to appreciate the societal merit of non-state money. The gross and systematic distortion of price signals caused by costless and arbitrary monetary inflation creates malinvestment, economic inefficiencies, and waste on a scale that would dwarf Bitcoin's approximate 0.05% share of global energy consumption.

The Bitcoin network provides a globally-inclusive, censorship-resistant, incorruptible, self-sovereign monetary network for the entire world. Within that context, the amount of energy used (again, 0.05% of the global energy) is absolutely worth the cost. Especially considering,

- nearly everyone on the globe is currently living under double-digit inflation
- Two billion+ people live under authoritarian regimes where their rights are suppressed and are subjected to capital controls
- 3 billion+ are underbanked or have no access to bank accounts

Bitcoin gives BILLIONS of people an alternative currency/savings technology where there otherwise are no alternatives. To claim Bitcoin has no utility or value is to deny the lived experience of millions **of less fortunate individuals cut off from the Western world's living standards and freedoms.**

Note the chart below from Chainalysis, which attempts to rank crypto usage/adoption by adjusting for things like population, wallets, purchasing power, etc. for more representative comparison of actual adoption. This is a list almost entirely of emerging economies and countries in distress. While the citizens of Pakistan, Nigeria, Argentina, and others may not have billions to convert into cryptocurrencies, even their small purchasing power is being protected thanks to cryptocurrencies.

TABLE 1:
Top 20 most crypto-active countries - Chainalysis Global Crypto Adoption Index

RANK	COUNTRY	OVERALL INDEX RANKING[1]	RANK	COUNTRY	CRYPTO ADOPTION INDEX[1]
1	Vietnam	1.00	11	Colombia	0.19
2	India	0.37	12	Thailand	0.17
3	Pakistan	0.36	13	China	0.16
4	Ukraine	0.29	14	Brazil	0.16
5	Kenya	0.28	15	Philippines	0.16
6	Nigeria	0.26	16	South Africa	0.14
7	Venezuela	0.25	17	Ghana	0.14
8	United States	0.22	18	Russia	0.14
9	Togo	0.19	19	Tanzania	0.13
10	Argentina	0.19	20	Afghanistan	0.13

1. Chainalysis combines three measures of crypto usage and adjusts these for market purchasing power (on-chain cryptocurrency value received, On-chain retail value transferred, Peer-to-peer (P2P) exchange trade volume).

Source: 2021 Chainalysis Global Crypto Adoption Index

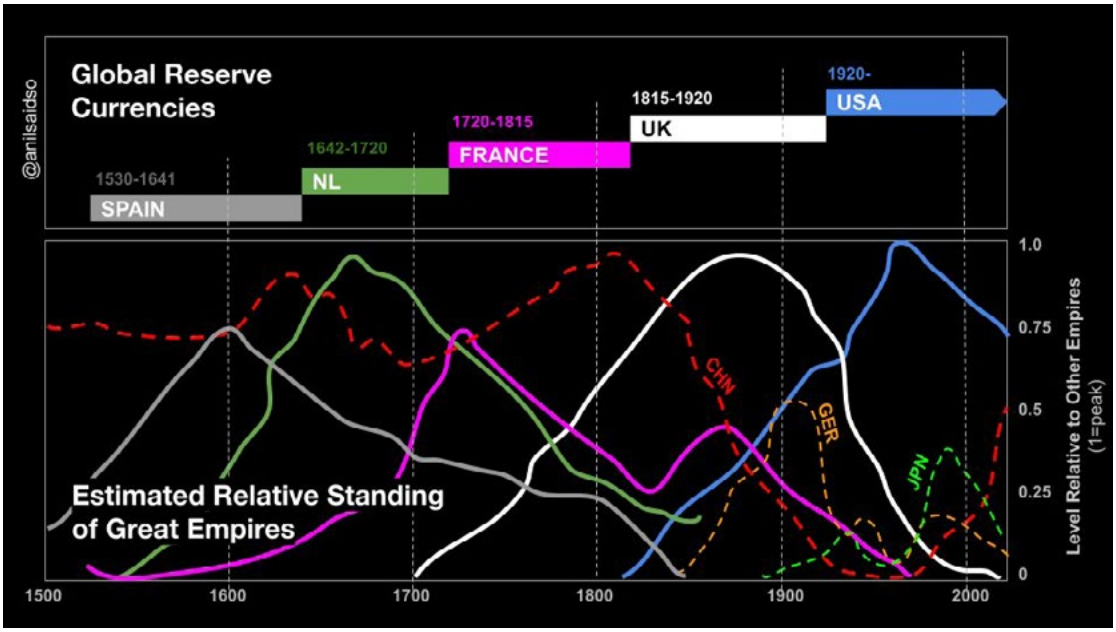
Source: Coinshares and Chainalysis

But My Financial System Works Great

"It is well enough that people of the nation do not understand our banking and monetary system, for if they did, I believe there would be a revolution before tomorrow morning."

- Henry Ford

We touched on fiat money initially, but it is worth revisiting just how new and flimsy the idea of "money backed by the government's word" really is. Historically, most currencies were pegged to scarce physical commodities such as gold or silver, but today, fiat money is backed by neither anything physical nor scarce. Since it is not linked to any physical reserves (or based on math like in the case of Bitcoin), fiat is subject to artificial manipulation, experimentation, and adulteration. One of fiat's biggest risks is becoming worthless due to hyperinflation, a scenario that has played out **repeatedly** in history. If people lose faith in a nation's paper currency, like the U.S. dollar bill, the money will no longer hold any value.

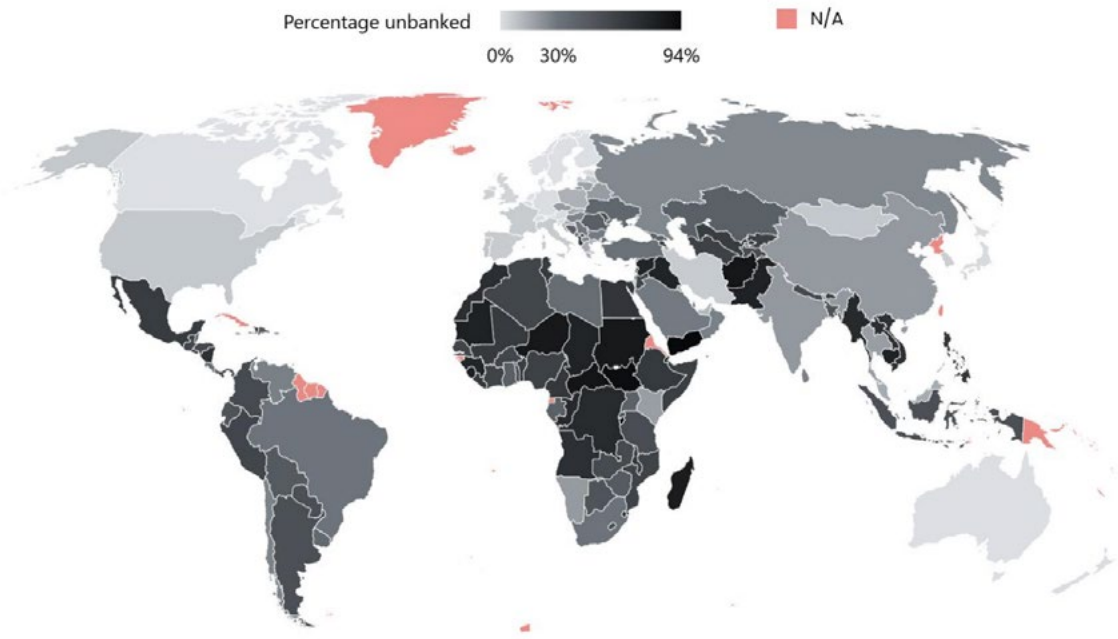


The rise and fall of global reserve currencies throughout time. Source: AnilSaidSo

Governments control fiat money and, throughout history, have frequently abused their control on the issuance of money. It is not hard to understand the consequences of a system in which a small minority controls the money for everyone. As Dergigi penned, "If you control the money, you control the purchasing power. Which, in turn, allows you to control most other things."

Government abuse and/or incompetence throughout history has led to the destruction of economies and money, oftentimes by hyperinflation. Infamous examples include ancient Rome, Weimar Germany, the Balkans and Zimbabwe in the 1990s, and present-day Argentina, Venezuela, Turkey, and Lebanon. Beyond that, 2B+ people across the world are considered "unbanked," meaning they do not have access to a bank account or banking services. These people have almost no way to save their money or provide for themselves beyond the day-to-day.

Figure S7 – The unbanked as a percentage of the population by country.



Source: World Bank Data

Utility Versus Emissions

Until now, we have only discussed Bitcoin's energy usage. However, when discussing climate impact, we must also consider:

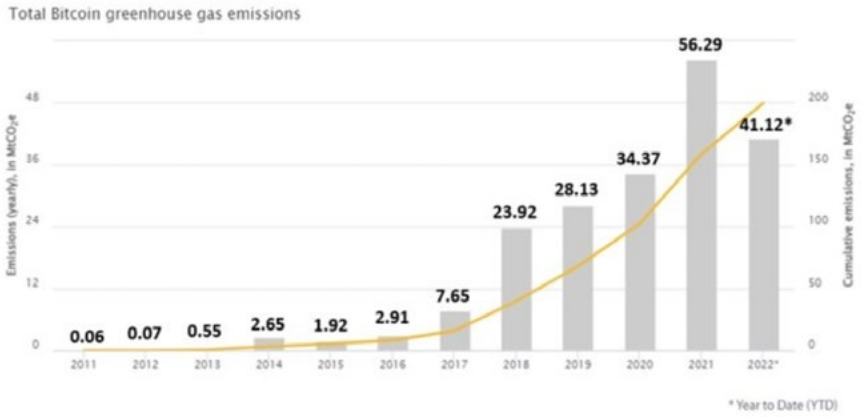
- What is the energy source?
- Is this energy that could be used elsewhere, or is it "stranded"?
- How does the energy mix compare to others?
- What are the actual emissions?

Actual Emissions

We'll touch on all these but let's focus on emissions for now as they are what ultimately matter, right? How does Bitcoin stack up to some other major industries?

According to the most recent report from the CCAF, annualized greenhouse gas (GHG) emissions have decreased considerably over the course of 2022. The CCAF estimates that Bitcoin mining is currently responsible for ~48 MtCO2e annually, down ~37% from its peak in Q2 2021. This decrease is primarily attributable to a fall in electricity usage as miner profitability has become strained in the crypto bear market.

The ~48 MtCO2e of annual GHG emissions from Bitcoin mining projected by the CCAF are a small part of the ~50,000 MtCO2e of annual GHG emissions worldwide (in 2019). The White House Office of Science and Technology Policy produced a paper a few weeks ago estimating that all PoW mining, including Bitcoin, contributes between 0.2% and 0.3% of global greenhouse gas emissions. Although the amount is not zero, it is considerably less than the sensationalized media headlines would have investors assume.

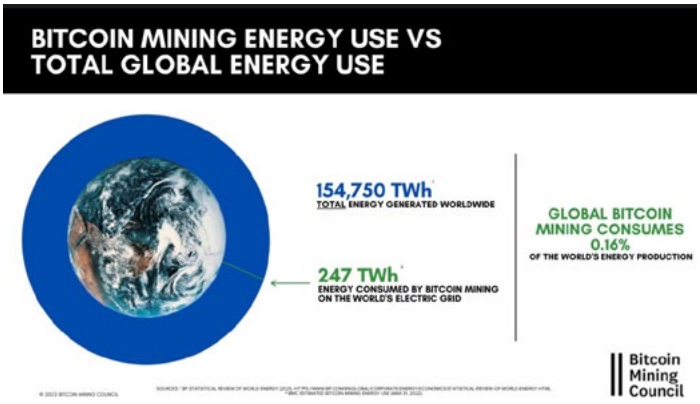


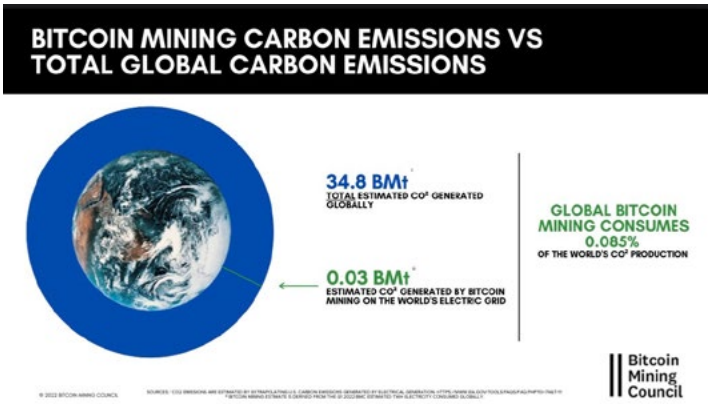
Remember, Bitcoin mines simply use electricity. "Green" energy can be used to mine Bitcoin, meaning fewer emissions for the same energy usage. The latest CCAF estimates are that the Bitcoin network is powered by ~38% of renewable energy from its energy mix. Bitcoin's security is ultimately entirely generated from electronic hardware and electricity, which is much easier to decarbonize than some of the other means of securing currency. The U.S. military, instrumental in securing the value of the U.S. dollar, emits more Co2 than many industrialized nations.

Now that we have an idea of the ***absolute*** numbers surrounding BTC mining GHG emissions (~48 MtCO2e and ~0.2% of global emissions), let's provide some context and compare that in a relative sense to other industries. For one of the most straight-forward comparisons, the emissions resulting from the gold industry are estimated to be between 100 and 145 Mt of CO2 annually (2-4x of Bitcoin mining).

Galaxy Digital estimates the global banking system used 264 TWh of energy in 2019. Using the average global carbon intensity of 492 gCO2/kWh, CoinShares was able to equate this to 130 Mt of CO2 emissions per year (or ~3x Bitcoin mining).

Google consumed approximately 15 TWh of power in 2020 (~0.01%), the same order of magnitude as the Bitcoin network. Google's purported transition to renewable energy has astutely noticed the PR risk associated with its users thinking about how much energy is required in order to offer their service, with some estimates placing each search as about as energy-intensive as turning on a 60W light bulb for ~20 seconds. This ***transition to renewables*** is on the basis of Renewable Energy Certificates (RECs) rather than actually, say, generating clean energy and ***directly*** utilizing this to power Google's data centers.

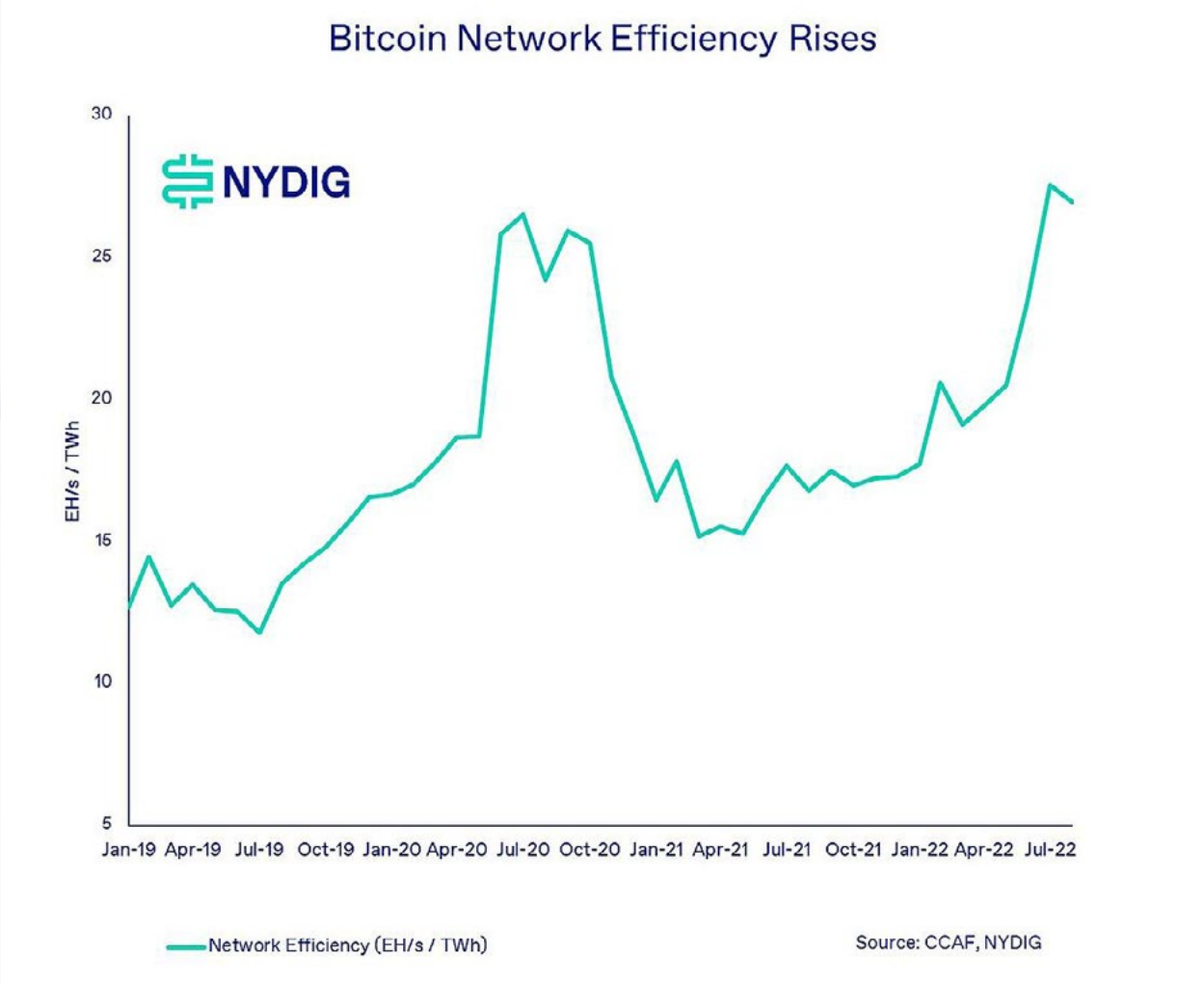




Nevertheless, this is a solid indicator of the social acceptability of maintaining highly energy-intensive industries, so long as their output is useful, valuable and perceived to be sustainable.

Network Efficiency

Bitcoin's energy consumption is increasing (on a long-term trajectory), but it is also growing more efficient. Despite a decline in electricity consumption in 2022, the network hash rate, which represents the combined computational effort of all network miners, remains near an all-time high in Q4 2022. This combination of decreased electricity use and increased hash rate has resulted in a more efficient network. One factor contributing to the efficiency gains miners have found it cost-effective to replace old, inefficient mining AISICs with new, more efficient ones.



Developers continue to find new ways to maximize Bitcoin's efficiency from a code and mining standpoint. One example is SegWit, enhancement introduced in 2017 that removed superfluous information from the transaction's code without compromising security. Today, SegWit transactions constitute the bulk of all network transactions.

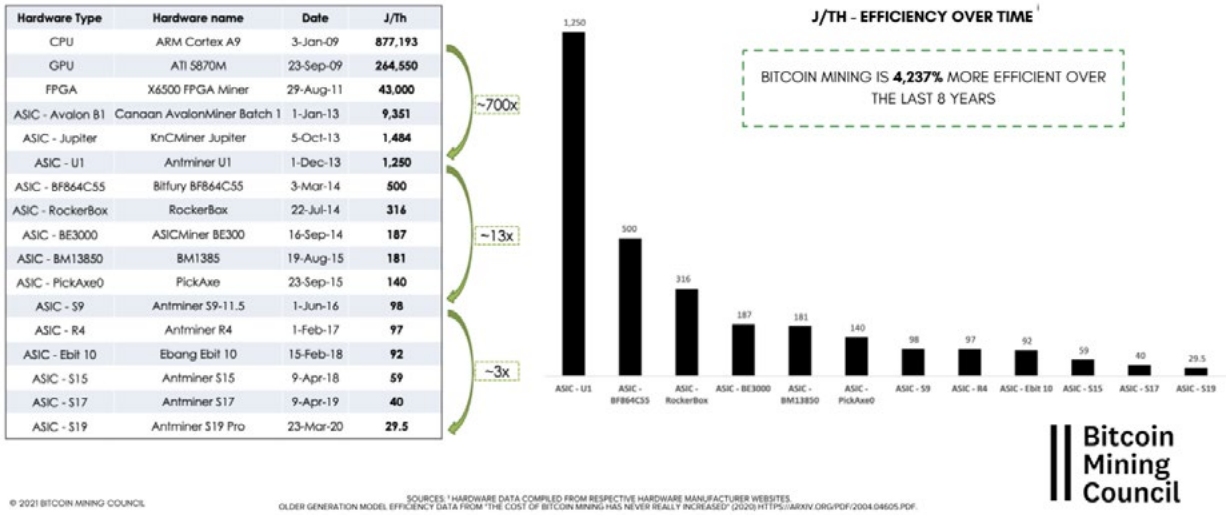
Source

Among other advantages, SegWit enabled the development of the Lightning Network, which enables Bitcoin payment channels that can execute millions of transactions between two parties with no additional mining hardware or costs.

Another area of optimization is in the mining hardware. Each newly manufactured ASIC still consumes electricity but is using the same amount of energy with increasing efficiency. The Antminer S19 is five times more efficient than the Antminer S9, which was manufactured only a few years earlier.

Network efficiency (average monthly hash rate divided by monthly electricity usage) can be conveyed with the ratio EH/s / TWh. This relationship is the amount of exahash produced by all Bitcoin miners per second divided by the terawatts per hour used to produce those exahashes. One of the biggest jumps in mining efficiency has been due to the semiconductor chips used in ASICs. As the chips find new ways of becoming more efficient, the mining industry should continue to improve in terms of hash rate per unit of energy usage, everything else being equal.

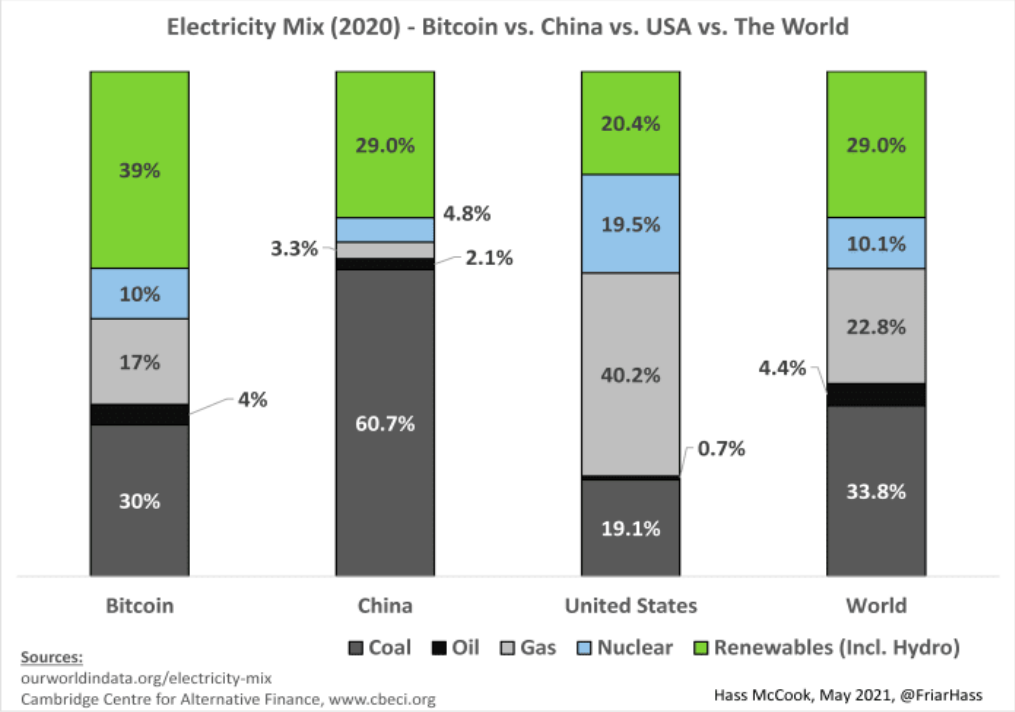
According to the Bitcoin Mining Council, Bitcoin mining has become ~5,800% more efficient over the past eight years. In other words, the economic value of a hash produced by a miner eight years ago is vastly different from that of a hash produced today. The council also determined that the average estimated Joules per Terahash (J/TH) of a typical machine is 48.9 J/TH, representing a roughly 200-fold increase in efficiency since the introduction of the first ASICs in 2013.



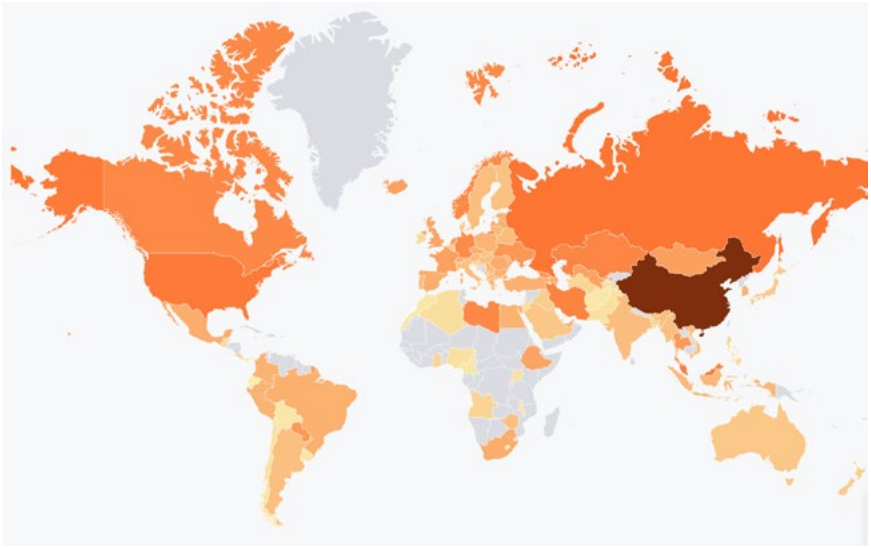
What About the Energy Mix?

In 2020 China provided approximately ~2/3rds of Bitcoin's overall hashrate, with the majority of this electricity being generated by burning coal. As of 2022, the Bitcoin network looks to be on a path to a greener future, with ~39% of the power used coming from renewables.

Maybe 39% does not sound like a lot? You may be thinking, Bitcoin can do better! Again, we'll emphasize context. How does Bitcoin, the global money, compare to other countries? Spoiler: it's "greener." Even the U.S., the most advanced, developed, affluent country in the world utilizes renewable energy at half the rate Bitcoin mining does.

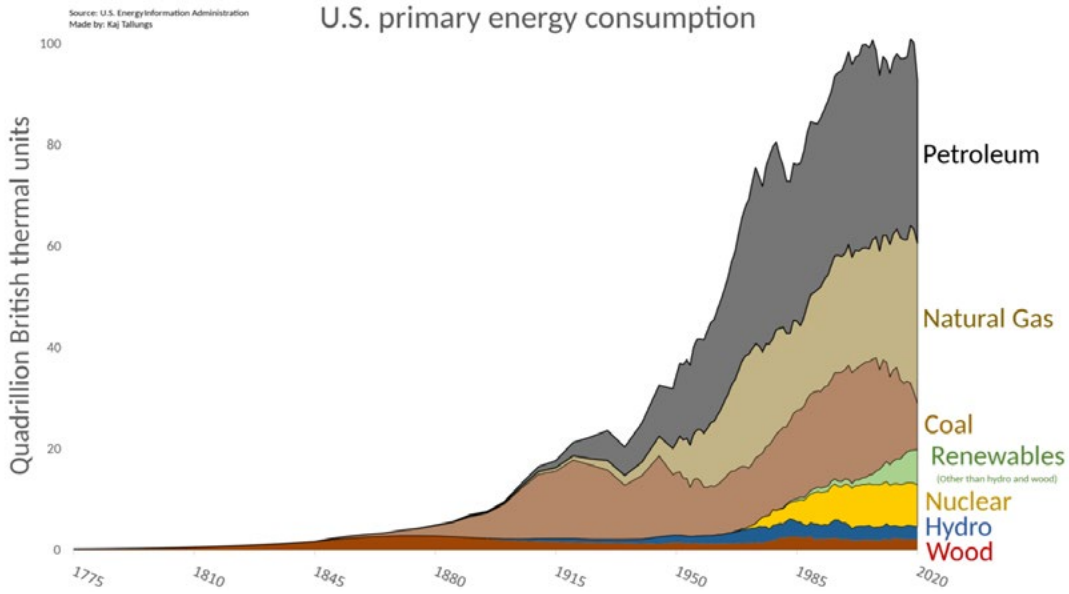


Additionally, where Bitcoin sources its energy has only improved since the above chart was created. Before May 2021, China contributed a sizable portion to Bitcoin's emission totals. Per CoinShares, in 2020, China contributed upwards of 65% to Bitcoin's carbon intensity.



Bitcoin Hashrate Global Geographic Distribution Source: cbeci.org

However, in May 2021, all that changed when China outlawed bitcoin mining and miners began shutting down throughout the country. While this was a shock to the network in the short term, the silver lining was that many of those Chinese miners would have to relocate somewhere else, most likely "greener" places. And in fact, many relocated to the U.S., which uses far less coal-powered energy sources than China.



Source

A Note on Transaction Throughput & Performance

Many Bitcoin critics often claim that each Bitcoin transaction requires the same amount of energy as would be required to power a typical house in the U.S. for six weeks (or a similar outlandish comparison). Such claims fundamentally do not understand how the Bitcoin network works. An individual Bitcoin transaction does not have a particular energy requirement, nor does adding more transactions require more energy. This relationship does not exist. In fact, most of these "reports" claiming to cite a widely debunked "academic paper" were later revealed to be a 2-page report written by college undergraduates as a class assignment. We highlight this to drive home the point of just how minimal effort mainstream detractors put into understanding Bitcoin.

As Cambridge University's Center for Alternative Finance explains, the number of transactions the Bitcoin network can process is independent of energy use. Adding more hash power to the network (using more electricity) won't increase the protocol's transaction throughput. In the opposite way, processing more transactions does not require additional energy consumption. The hash power is the total security over the network. More hash power means Bitcoin is more secure, which means users can have more confidence in storing and transacting in the Bitcoin network.

The Bitcoin network hash power is (crudely) akin to a vault for regular money. The vault is a big, expensive barrier to keeping your money safe. However, you do not have to add more steel every time you add another dollar to the vault. The vault can handle $1 or $100 million with the same security budget.

Also, not every transaction on the Bitcoin network is the same. As mentioned, the Lightning Network enables one transaction on the Bitcoin network to include thousands (or even millions) of individual payments to and from people. Similarly, tools like OpenTimestamps enable linking potentially billions of data points to a bitcoin transaction.

"This isn't just speculative. It's happening today. As Fedwire's 800,000 or so daily transactions reveal little about the total payments volume supported by the network, Bitcoin's 300,000 daily transactions and 950,000 outputs do not tell the whole story." –"The Frustrating, Maddening, All-Consuming Bitcoin Energy Debate," Nic Carter

This is precisely how traditional payment networks of today have scaled. The Bitcoin network is a final "cash" settlement layer without needing a trusted party. Often, Bitcoin is compared to, or described as it is competing with, payment processor companies like Visa in facilitating global payments. While it does facilitate payments, this comparison is flawed in many regards.

High-performance retail ***payments networks***, like PayPal or Visa, do not offer final settlement between banks — they are credit-based systems that rely on a monetary base layer of central banks for final and irreversible settlement. In fact, all legacy retail payment systems, including traditional banking, are layered (see here).

Bitcoin is more sensibly comparable to base money: fiat money like the USD, Euro, Yuan, and others, as well as gold. Gold is the base money of the past, while government fiat is the current base money. Fiat base money includes the physical cash (bills and coins) and, more importantly, the digital accounts/reserves held at the central bank. These represent the final settlement between parties, while all other monetary measurements (M1, M2, M3, etc.) represent claims on other money or someone else's debt.

When discussing the "performance" of the Bitcoin blockchain, one must consider the time, trust, and costs involved in a transaction. Bitcoin facilitates trustless peer-to-peer transactions with a truly digital bearer instrument. Performance is measured in 2 ways:

- Throughput: The number of transactions the system can process per second.
- Latency: The time it takes for a transaction to be processed.

Trust can be measured along a spectrum, but here we'll divide it into two parts again.

- Low Trust: anyone (including Bitcoin users) can run node software to independently compute the latest state and verify that all rules in the system were followed. Each user can check, at any time, that there has been no fraud, no cheating, no rule changes, etc.
- Low Cost: If the node software is expensive to operate, individuals will rely on trusted third parties to verify the state.

Where Bitcoin truly outperforms is in trust and cost. There is no counterparty risk associated with Bitcoin. No bank freezes, banking limits, transaction censorship, fractional reserve lending, or bank insolvency risk. While Bitcoin's transaction throughput and latency aren't enticingly competitive with Visa, its settlement times measure quite favorably to actual banks or remittance payments.

Bitcoin is the equivalent of giving someone a $20 bill. Once it has traded hands, you own it. It is in your control, and no bank or government was required to facilitate that transaction. Now, imagine doing that at any time, with anyone, anywhere, for any amount of money. Banks have numerous downsides but sticking to actual transfer times, they take days to settle via SWIFT. Remittance payments can take weeks!

Bitcoin completely replaces central banks' real-time gross settlement (RTGS) base layer with a global and neutral monetary settlement network. If one wants to compare payment systems accurately, the media and academics should be comparing Bitcoin to the transactions of central bank RTGS systems — and include the impact of the militaries and institutions that legitimize them. Bitcoin is most accurately compared to Fedwire in the United States and TARGET2 (the successor to TARGET) in the Eurosystem. Retail payment systems can and will plug into Bitcoin the same way they do with permissioned state-sponsored systems.

Empower 2023

Energizing Bitcoin

March 7–9, 2023

Bringing Bitcoin Mining to the World's Energy Capital

Empower is the only bitcoin mining event with a focus on energy — bringing together energy, mining, finance, and other professionals in the city that powers the world.

Take over Downtown Houston with Digital Wildcatters for an iconic three-day event to learn and network with energy producers, capital groups, miners, and other builders in the space.

Empower brings the most forward-thinking names together to speak on topics such as natural gas and renewable mining, power generation, venture capital, institutional adoption, regulatory, and more.

The Empower audience is an impressive mix of entrepreneurs, energy pros and crypto experts. In 2022, attendees included companies from Riot Blockchain, Bloomberg, Asic Jungle, Compass Mining, Google, ExxonMobil, Foundry, J.P. Morgan Chase, Talen Energy, and so many more.

The Digital Wildcatters believe in getting smart people together and allowing collisions to happen — collisions that catalyze ideas, collaboration, and progress. You will have the opportunity to hang out with other like-minded people in a fun environment with live music, networking parties, and free beer.

By The Numbers

1000+
Attendees

3
Days

24
2022 Corporate Sponsors

Empower is the only bitcoin mining event with a focus on energy — bringing together energy, mining, finance, and other professionals in the city that powers the world.

80
Speakers

DIGITALWILDCATTERS

About CRYPTOEQ

CryptoEQ™ is an independent digital asset analysis and rating agency that provides unbiased, objective, and transparent research you can trust. We help people navigate their investment journey and trading decisions.

Spencer Randall
Principal & Co-Founder

- 8+ Years in System Architecture Implementation
- 5+ Years in Crypto Trading/ Investing
- Bachelor of Science in Engineering

Brooks Vaughan
Head of Innovation & Co-Founder

- 17+ Years in Product Design/ Management
- 8+ Years in Crypto Trading/ Investing
- Bachelor of Industrial Design

Michael Thoma
Lead Analyst & Co-Founder

- 11+ Years in Technical Research/Analysis
- 5+ Years in Crypto Trading/ Investing
- Master of Science in Geology

Company Statistics

+85%
Algorithm Win Rate

+175%
Average CORE Rating ROI

+340%
Y/Y Revenue

+100,000
Total Active Users

We help you gain the market insights you need to grow your cryptocurrency portfolio. Our team's supportive and interactive approach helps you refine your crypto investing and trading strategies.

We provide research and analysis for quickly-evolving blockchain technologies to make navigating the digital asset class less intimidating. Our research encourages informed decisions for long-term investments or short-term strategies.

Our proprietary algorithms, exhaustive research and helpful community are key to our success as we follow strict principles and ethics to deliver honest information. We actively seek to identify scams and low quality nefarious projects relieving you of that burden.

Platform Highlights

v1 launched in 2019

» Signal over noise.

» Direction over data.

» Quality over quantity.

» Usability over complexity.

Final Words
Our Story

Like most disruptive tech startups, CryptoEQ started as a small group of like-minded people with a big idea.

Each of our co-founders—Spencer Randall, Michael Thoma and Brooks Vaughan—were cryptocurrency investors and traders before the crypto explosion of 2017. They met attending local crypto conferences and immediately began to admire each other's perspective and maverick approach to the assets available on the market. After seeing one another in action, they each noticed a glaring hole in the crypto-asset market—truly unbiased, thorough insights and deep research.

In July 2019, we launched CryptoEQ and acquired approximately 3,000 new users—so we set a goal to continually rethink our products. CryptoEQ v2 debuted in January 2020 with new all features. Our third iteration, v3, launched in June 2020 with an average quarterly revenue growth of over 300%. We also blew through our 5,000-user milestone. v4 incorporated a new and intuitive user interface and exclusive 1-on-1 bespoke solutions pushing us past 50,000 users. v5 was on track to exceed 75,000 users, but markets move fast, so we pushed v6 live September 1, 2022. We also upped our target to hit 100,000 users by 2023.

Need More? Reach Out!

Refine your trading and investing strategy to make optimal decisions. We help you gain the market insights you need to efficiently manage your exposure across a variety of digital assets.

Our enterprise solutions help your company leverage our teams' collective three decades of experience investing and trading digital assets. Whether it's publishing key sector-specific reports, end-to-end solutions, or data licencing, our teams can take on your research efforts to produce an institutional-grade report for your audience. All of our sessions are scheduled for direct face time with CryptoEQ Co-Founders and Partners. With each session, you have the option to schedule either a virtual experience or an in-person experience at one of our Houston-area offices. So if you need a deep dive on a specific asset or a broad re-balancing of your portfolio—we can remove your research bottleneck!

DIGITALWILDCATTERS

CRYPTOEQ

Bitcoin Mining:
A Global Economic Perspective

CryptoEQ CORE+ Series

Contact

Team@CryptoEQ.io

Houston, Texas

United States

CryptoEQ.io