# Cryptocurrency Mining
## *A Primer*

April 2019

### INTRODUCTION

On January 3, 2019, cryptocurrency mining, specifically bitcoin mining, celebrated its tenth anniversary. A decade ago, mining was little more than a niche hobby for a small group of cryptography enthusiasts with a desire to support a radically innovative currency. Today, crypto mining has become a burgeoning enterprise, complete with complex, specialized equipment and dozens of stakeholders, from semiconductor manufacturers to regional utilities.

We often hear that mining is one of the more difficult concepts to tackle in the crypto industry, particularly for newcomers. This primer is intended to demystify the complexity of mining through an introductory-level explanation. In order to provide you with a comprehensive and detailed understanding, we've chosen to focus on the intricacies of bitcoin mining, with references to other crypto protocols along the way.

We'll begin with a brief description of crypto mining and its role in validating blockchain transactions. Then we'll discuss the key steps required to mine a valid block as well as some of the major players involved. Lastly, we'll conclude with an overview of the economics of mining, including a framework for measuring profitability, perspectives on the ecological externalities, and a brief summary to bring it all together.

## Table of Contents

# I. Concepts

Cryptocurrencies represent a significant advancement in financial and economic inclusion, relying on the tenets of internet communication and cryptography. A key theme of the crypto industry is the concept of decentralization, or the lack of a single point of failure. A properly decentralized network is unlikely to fail just because a single individual, group of individuals, or company decides to no longer participate in the network, either voluntarily or through compulsion. This means that well-designed crypto protocols, like bitcoin, are highly robust and secure. Decentralization provides a number of other benefits, including: censorship resistance, transaction immutability, bearer claim and/or proof of ownership, financial mobility, and improved privacy, to name a few.

In order to operate a decentralized transaction network, however, individuals need to trust a method for reliably validating transactions without depending on single points of failure. Building this trust on top of a "trustless" network of computers is an inherently difficult problem, but one that Satoshi Nakamoto, the pseudonymous author of the bitcoin white paper, creatively challenged. Nakamoto's innovation is a validation process colloquially referred to as "**mining**."

Crypto mining is the process of adding a **block**, or a collection of transaction data, onto a **blockchain**, or a complete record of all transactions on a particular protocol. Blocks contain metadata that reference predecessor blocks, forming a chain structure. Attempts to alter a single link on the chain produce an invalid result and are therefore rejected by the broader network.

Participants engaged in mining, or "miners," validate transactions by using computational equipment to solve a puzzle, each time looking to add a single block onto the chain.[1] Their reward may include a combination of new coin supply, called a block reward, and transaction fees, also known as network fees. This reward depends significantly on the unique design of each crypto protocol; some, by design, do not reward miners through inflation or transaction fees.

Like fiat money, many crypto protocols are subject to inflation through block rewards issued to miners. As miners validate transactions and introduce new blocks to the chain, they grow the total currency supply. Notably, though, fiat money supply is often managed by a central bank, whereas most crypto supply is subject to a codified inflation rate. This means that as long as a protocol's software is free of bugs, the inflation rate is highly predictable and cannot be managed or manipulated by a single participant.

Mining evidently plays a very important role in maintaining the integrity of a crypto protocol and, in many cases, the total currency supply. In the next section, we'll break down the process of proof-of-work ("PoW") mining on the bitcoin protocol and provide a brief introduction to proof-of-stake ("PoS") forging.

1 The term "miner" is derived from the bitcoin whitepaper. "The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation." Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf)

# II. Process

The complexity, cost, and effort involved in crypto mining safeguards a protocol from adversarial participants and double-spending. Honest miners are vital towards ensuring legitimate transaction settlement, providing bookkeeping services to the network, and introducing newly minted coins into the market.[2] In this section, we touch on the process of mining on the bitcoin protocol, step-by-step.

Before delving into the details, first let's cover the concept of a **hash**. A hash is a string, or a series of numbers and letters, oftentimes fixed in length. Hashes are outputs of a hashing algorithm, a mathematical function that takes a random input and results in a unique output.

The bitcoin protocol utilizes **Secure Hash Algorithm-256**, also known as SHA-256. SHA-256 is a cryptographic function applied to an input to generate a number displayed as a **hexadecimal number**. It is cryptographic in the sense that each output is unique to an input, much like a public-private key pairing. Only the individual with knowledge of the input (the private key) will be able to produce the same output (the public key). Minor alterations to the input results in a completely different output, as figure 1 demonstrates below.[3]

**Figure 1: Example of hashing via SHA-256**

| Input | Output (SHA-256 hash) |
|---|---|
| Bitcoin | b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4 |
| Bitcoin is a peer-to-peer | 92c3406a275de62ecb23cf6b0dfed293cc0e8196d8aa8db4e392a4c93cff6040 |
| Bitcoin is a peer-to-peer electronic cash system that allows participants to digitally transfer units of bitcoin without a trusted intermediary. | 185be86643186c8bdda19c06b350b9d910b03a6e85aad265ca540cc24cafd7ea |
| Bitcoin is a peer-to-peer electronic cash system that allows participants to digitally transfer units of bitcoin without a trusted intermediary. Bitcoin combines a public transaction ledger (blockchain), a decentralized currency issuance algorithm (proof-of-work mining), and a transaction verification system (transaction script). Bitcoin has a supply cap of 21 million bitcoin, 95% of which will be mined by the year 2025. Bitcoin relies on Nakamoto consensus, or consensus implied by the longest blockchain that has accumulated the most computational effort. | 4608769961da2b18ba8d27257df50788f448631489ce558945ae946c060f3252 |

*Source: Kraken Intelligence, SHA-256 Hash Generator*

Hashing algorithms have several attractive properties, including:
1) uniqueness of an output hash;
2) unidirectional algorithms; and
3) the fixed output length.

With respect to uniqueness, the same input will always yield the same exact output. Hash algorithms are unidirectional and nearly impossible to reverse engineer. Trying to find the input string used to derive a hash requires brute force guessing, which could theoretically require lifetimes of dedicated computational effort. Finally, fixed output lengths are a more efficient method for storing data. As figure 1 demonstrates, despite longer inputs, the hash is always 64 characters in length.[4] While the bitcoin protocol leverages SHA-256, other cryptocurrencies may rely on different hashing algorithms. For example, ethereum utilizes the **Ethash** algorithm. Conceptually, the same benefits of hashing still apply across other algorithms.

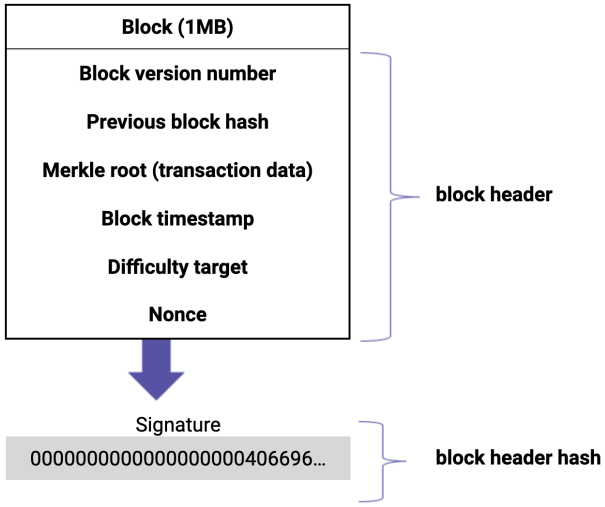
Now that we've considered hashes, let's move on to blocks.

2 "Decoding the enigma of Bitcoin Mining - Part I: Mechanism," Kiran Vaidya (https://medium.com/all-things-ledger/decoding-the-enigma-of-bitcoin-mining-f8b2697bc4e2)
3 Test hashing via SHA-256 for yourself at the following, free hash generator: https://passwordsgenerator.net/sha256-hash-generator/
4 "Cryptographic Hash Functions Explained: A Beginner's Guide," Daniel Pigeon (https://komodoplatform.com/cryptographic-hash-function/)

We previously referred to blocks as a collection of transaction data, which are subsequently linked to each other in a chain. In order to better grasp this structure, let's cover the key elements that make up a block in the bitcoin protocol. Most blockchain protocols leverage a similar block structure. As illustrated in figure 2, bitcoin blocks contain the following elements:[5]

- the block version number;
- the previous block hash;
- the merkle root;
- the block timestamp;
- the difficulty target; and
- a nonce.

**Figure 2: Bitcoin block structure**




*Source: Kraken Intelligence*

The **block version number** indicates the version of the bitcoin software a miner is running on their full node, which allows other network participants to track upgrades or changes to the protocol, including which consensus rules to follow.[6]

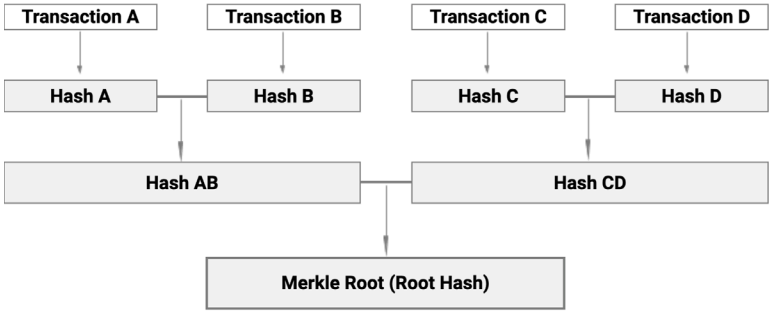
The **previous block hash** is the hash of the preceding block header, which directly links successive blocks and prevents invalid alterations of transaction history on the main chain.[7]

The **merkle root** is a hash of a block's **merkle tree**. In a merkle tree, all transactions are condensed into a binary tree-like structure for efficient storage.[8] Then, transactions are hashed together recursively using SHA-256 until the process results in one final hash: the merkle root.[9] This process is illustrated in figure 3.

The **block timestamp** is the number of seconds elapsed since January 1, 1970, also known as UNIX time.[10]

The **difficulty target** of a block is a hexadecimal number beginning with a consecutive number of zeros, or leading zeros. The hash of a block header must meet the difficulty requirement for the network to validate the block. Meeting this difficulty target requires producing a hash with the same or more leading zeros than the target. The difficulty target adjusts every 2,016 blocks to ensure that blocks are added every ten minutes, on average. An increase in the difficulty target requires exponentially more effort from miners in order to generate a valid block.

**Figure 3: Deriving a merkle root**




*Source: Kraken Intelligence*

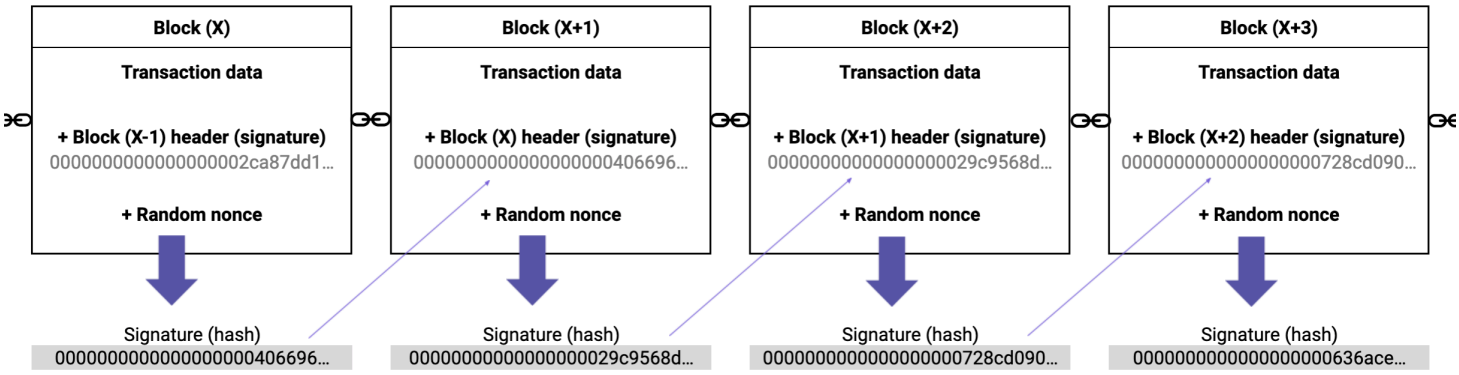
A **nonce** is an arbitrary number that is used once and then incremented, or adjusted by 1, after each attempt to produce a valid hash.

All of these elements are combined into an input string and subsequently hashed twice[11] to generate an output known as the **block header hash.**

5 Block header breakdown provided by the Bitcoin Developer Reference on bitcoin.org (https://bitcoin.org/en/developer-reference#block-headers)
6 "The block version number indicates which set of block validation rules to follow." Bitcoin Developer Reference (https://bitcoin.org/en/developer-reference#block-headers)
7 "A [SHA256 hash]... of the previous block's header. This ensures no previous block can be changed without also changing this block's header." Bitcoin Developer Reference (https://bitcoin.org/en/developer-reference#block-headers)
8 See merkle tree construction provided by the Bitcoin Developer Reference https://bitcoin.org/en/developer-reference#merkle-trees)
9 "A [SHA256 hash]... The merkle root derived from the hashes of all transactions included in this block." Bitcoin Developer Reference (https://bitcoin.org/en/developer-reference#block-headers)
10 "The block time is a Unix epoch time when the miner started hashing the header (according to the miner)." Bitcoin Developer Reference (https://bitcoin.org/en/developer-reference#block-headers)
11 Hashing twice makes the mining process resistant to length extension attacks (https://crypto.stackexchange.com/questions/3978/understanding-the-length-extension-attack)

By virtue of hashing all of this metadata together and subsequently linking blocks in succession, we can see that a blockchain is a robust architecture that prevents even minor alterations to transactions stored within an individual block. A simplified view describing how each block impacts the evolution of the blockchain is presented as figure 4 below.

**Figure 4: Blockchain architecture simplified**




*Source: Kraken Intelligence*

So far, we've described what blocks are made of, but not how all of this transaction data is sourced or how valid blocks are propagated to other participants. Now, we'll discuss this gossip function in the context of the two primary block validation methods utilized by crypto protocols where mining (or forging) is relevant: proof-of-work and proof-of-stake.

**Proof-of-Work (PoW)**

Many crypto protocols, including bitcoin, require "proof-of-work," or expended computational effort, in order for the network to recognize a block as valid. Participating miners simultaneously compete against each other to provide a valid PoW, or a block hash that meets the difficulty requirement, in order to earn the **block reward** and related **transaction fees**.

The first step in PoW mining is for a miner to collect transaction data from a pool of unconfirmed transactions, known as the **mempool**. To prevent the inclusion of **double spend** transactions, which could invalidate the block, miners first filter for transactions included in the previous block and remove them from the mempool. Miners then package a set of remaining unconfirmed transactions and their associated metadata into a block, determine the merkle root, and begin the process of hashing block headers. Hashing is a game of speed and luck. If a miner hashes a block header that does not meet the difficulty target, the miner will increment the nonce and continue testing their luck. Similar to the SHA-256 demonstration in figure 1, even the slightest change to the nonce will result in a completely different block header hash.

Once a valid PoW is discovered, the miner will propagate, or gossip, the details of the valid block to all other participating computers on the network, known as **nodes**. Nodes will independently verify that the presented block is valid, and if the network is able to establish consensus, all nodes will accept the new block into their record of the blockchain. The miner who successfully propagates a valid block will receive any block reward and associated transaction fees as part of the **coinbase**, or the first transaction included in each block directed to the miner's address. The coinbase may also be referred to as a generation transaction.[12]

In some cases, two or more miners may produce a valid PoW at similar times, resulting in a temporary, naturally occurring **blockchain fork**.[13] At this point, the race is on! Miners will compete to ensure that their block is not rejected as a **stale block**.

Imagine two blocks - block A and block B - are broadcasted at the same time and accepted by various nodes in the network. The miners responsible for block A and block B know that they have limited time to make sure their block isn't rejected, which will cost them their reward. Each miner will work as fast as they can to mine a successor block that will result in their branch of the blockchain

12 "A special field used as the sole input for coinbase transactions. The coinbase allows claiming the block reward and provides up to 100 bytes for arbitrary data." Bitcoin Developer Documentation (https://bitcoin.org/en/glossary/coinbase)
13 A fork may occur "when two or more miners find blocks at nearly the same time." Bitcoin Developer Documentation (https://bitcoin.org/en/glossary/fork )

being accepted as the **main chain**. If a miner introduces a valid successor to block A and propagates this PoW to the rest of the network, the fork that contains block A will be recognized as the main chain and the miner responsible for block A will retain their reward. Nodes that initially accepted block B will revise their record of the blockchain to exclude block B as a valid, yet stale block. Unfortunately, transactions included in block B are no longer considered confirmed.[14] Ultimately, the blockchain with the most accumulated proof-of-work, or the chain with the largest number of blocks, is considered valid by consensus. Consensus determined by accumulated proof-of-work is referred to as **Nakamoto consensus**.

Stale blocks are interchangeably referred to as **orphan blocks**, though they are slightly different concepts. Orphan blocks are valid blocks with an unrecognized parent block header hash. They are often the result of latency among geographically dispersed nodes. In some cases, groups of nodes "skip a generation" and receive communication of a block that meets the difficulty requirement, but that cannot be validated as no record of the parent block exists on these impacted nodes. This is a primary driver for the decision to use 10 minute **block times** on the bitcoin protocol, which provides nodes with ample time to communicate amongst each other as each block is mined. Some protocols, like ethereum, have far shorter block times, which result in higher orphan rates.

As blocks are added to the blockchain, valid transactions included in these blocks are said to have received **confirmations**. The number of confirmations represents how deep a transaction sits in the blockchain. For example, if a given transaction is included in block 10 and the **block height** of the most recent block is 20, the transaction is said to have received 10 confirmations. Every time a node accepts a new block as valid, it implicitly accepts all previous blocks (and their embedded transactions) as valid. This is because alterations to transaction histories require changes to all subsequent blocks in order for a malicious miner to successfully double spend. A transaction with a higher number of confirmations is therefore considered safer from malicious attempts to alter transaction history.

**Proof-of-Stake (PoS)**

A popular alternative to PoW validation is known as "proof-of-stake" (PoS). Under PoS, blocks are said to be **forged** or **minted** rather than mined. Forgers are also referred to as validators or stakers. Participating in PoS forging requires nodes to first stake a portion (or all) of their available crypto balance in a bound wallet, waiting to be selected as the next forger.[15] Unlike PoW networks, where miners amass computational resources to hash more quickly, PoS assigns the right to create a block through a lottery process. This lottery process is weighted by each participant's proportionate stake; staking nodes with larger balances have a higher chance of being assigned the right to forge. In essence, PoS relies on participants' staked coin supply to assign validation rights and drive consensus, whereas PoW relies on brute force computational power for validation and consensus.

Rewards from PoS forging may include block rewards and/or transaction fees. Because chosen stakers are given exclusive rights to create a block, protocols must include measures to counteract malicious attack vectors. Ethereum's proposed PoS concept, Casper, does so by confiscating staked cryptocurrency from stakers who attempt to validate incorrect transactions. These stakers are also barred from future staking activities.[16] PoS protocols are also unique in that they require an initial distribution of coin supply to allow participants to stake at genesis, typically through an **ICO** or an **airdrop**.[17] Other networks, similar to ethereum, have instead chosen to transition from PoW to PoS mining, which presents an alternative to conducting an ICO or an airdrop altogether.[18]

As we covered in this section, mining is a highly technical, yet integral process in the formation, validation, and maintenance of transaction histories on blockchain protocols. Understanding the elements of a block and the process of adding blocks to a blockchain provides us with a conceptual foundation for crypto mining in general. But perhaps as important as the technical details, the mining ecosystem relies on a diverse group of stakeholders to bring code to life.

14 Propagation Speed and Orphan Races, "Bitcoin Network Capacity Analysis - Part 6: Data Propagation," TradeBlock (https://tradeblock.com/blog/bitcoin-network-capacity-analysis-part-6-data-propagation)
15 "PoW vs. PoS: a comparison of two blockchain consensus algorithms," edChain (https://medium.com/@EdChain/pow-vs-pos-a-comparison-of-two-blockchain-consensus-algorithms-f3effdae55f5)
16 "PoW vs. PoS: a comparison of two blockchain consensus algorithms," edChain (https://medium.com/@EdChain/pow-vs-pos-a-comparison-of-two-blockchain-consensus-algorithms-f3effdae55f5)
17 "What is Proof of Stake?" Shaan Ray (https://hackernoon.com/what-is-proof-of-stake-8e0433018256)
18 Note that ethereum did conduct an ICO. Reference to ethereum in this comment is strictly with respect to the intent to transition from PoW to PoS

# III. Players

A myriad of individuals and entities in the mining industry are responsible for validating and securing a large number of blockchain protocols. In this section, we highlight some of the major constituents, a geographic dispersion of mining activity, and the importance of miner diversity.

A critical group of stakeholders in the mining industry are equipment manufacturers. The largest crypto mining equipment manufacturers include the likes of Bitfury, Bitmain, Canaan Creative, and Innosilicon. Currently, Bitmain leads the market for ASIC mining equipment, both in terms of unit sales and production capacity. Bitmain also has interests in several of the top mining pools. Bitfury similarly produces mining equipment and hosts their own mining pools.

**Figure 5: Mining equipment manufacturers**

| | Bitfury | Bitmain | Canaan Creative | Innosilicon |
|---|---|---|---|---|
| **Founded** | 2011 | 2013 | 2013 | 2006 |
| **CEO** | Valery Vavilov | Jihan Wu (Co-founder)<br>Micree Zhan (Co-founder) | N.G. Zhang | Gordon Ao |
| **Headquarters** | San Francisco, US | Beijing, China | Beijing, China | Wuhan, China |
| **Estimated revenue (2017)** | $93.7M | $2.5B | $179M (¥1.2B) | n/a |
| **Flagship products** | Bitfury Clarke<br>Bitfury Tardis<br>Blockbox AC | Antminer S9, S11, S15<br>APW 3++, APW7<br>Antrouter R1, R3 | AvalonMiner 911<br>AvalonMiner 851 | Terminator 3<br>Terminator 2 |
| **Supported algorithm** | SHA-256 | SHA-256, Ethash | SHA-256 | SHA-256, Ethash |

*Source: Kraken Intelligence, Coindesk, Bitfury, Bitmain, Canaan, Innosilicon, 8btc.com, craft.com*

Miners can be broken down by their participation and geographic location. We'll cover both solo and pooled mining methods, describe how mining resources are broken down geographically, and share insight into the importance of miner diversity and decentralization.

A **solo miner** is an individual participant looking to validate blocks alone. Under this operation, block rewards and transaction fees are credited to the single individual or entity. Major crypto protocols like bitcoin are not profitable for casual solo miners, though many altcoins still rely heavily on solo participants. Generally speaking, solo miners have been crowded out by the growth of larger mining groups, including pools. This evolution is most apparent in the bitcoin protocol, where solo miners initially handled all mining activity using personal computers. Over time, many of these miners were displaced by industrial-scale mining operations that employ specialized hardware.[19]

A **pool miner** is an individual engaged in mining through a collective, or a **mining pool**. Pool miners combine their hash rate as a group and split block rewards pro rata.[20] Generally, mining pools will define custom difficulty levels below network target difficulty, known as **share difficulty**. As pool miners hash block headers that meet the share difficulty level, they receive greater “share” of the mining pool. This is an effective method to gauge and track the contributions of individual miners in the pool. Once a valid block is produced that meets the protocol's target difficulty, the pool propagates the block and collects the reward. The pool then distributes the reward among pool members based on their share of the mining pool.

19 "A brief history of bitcoin mining hardware," Tristan Greene (https://thenextweb.com/hardfork/2018/02/02/a-brief-history-of-bitcoin-mining-hardware/)

20 "Three Countries With the Largest Number of Bitcoin Miners," iq option (http://forbes.ge/news/3175/Three-Countries-With-the-Largest-Number-of-Bitcoin-Miners )

In figure 6, we identify some of the benefits and limitations of both solo and pool mining efforts.

### Figure 6: Solo vs. pool mining

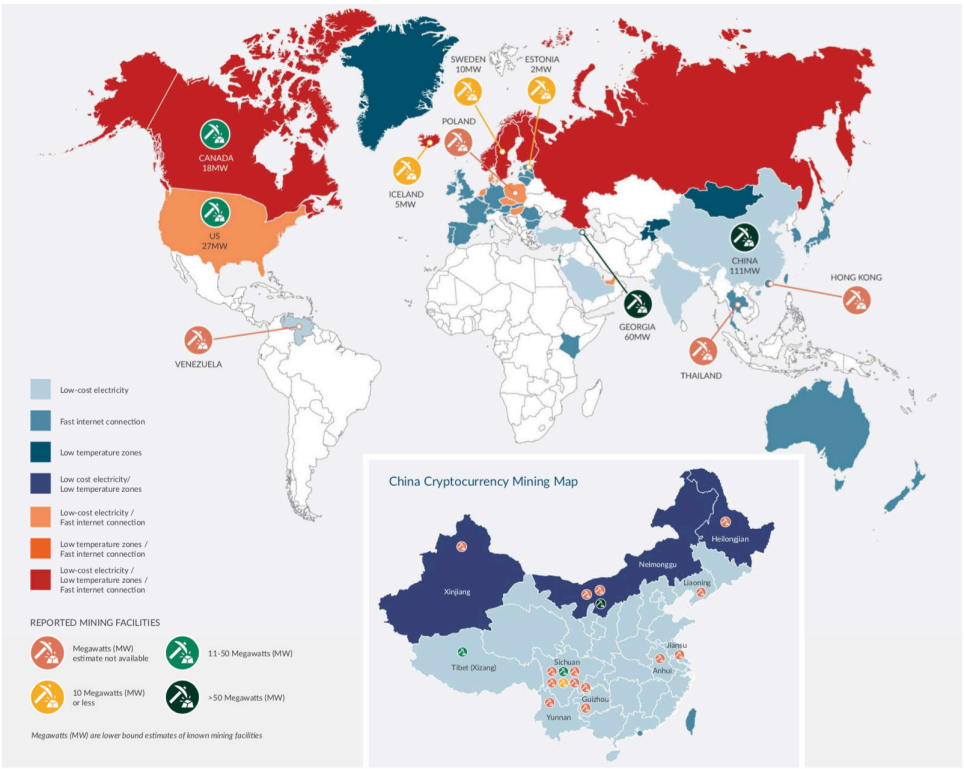
| | Solo Mining | Pool Mining |
|---|---|---|
| **Benefits:** | - Higher payout as rewards (block reward + tx fees) are directly credited to miner | - Steadier source of income due to higher frequency of mined blocks<br>- Continuous uptime in the event of singular node failure |
| **Limitations:** | - Inconsistent source of income<br>- Solely responsible for mining operations set-up and software/server security | - Higher risk of service-provider related interruptions (ie. DoS attacks)<br>- Mining pool fee is often charged to participating miners<br>- Transaction fees may not be distributed as reward |

*Source: Kraken Intelligence, Bitcoinwiki*

Regardless of whether a miner operates independently or in a pool, miners are constantly looking to increase output while reducing cost. The principal costs of running a mining operation include: 1) capital expenditure on dedicated hardware; and 2) electricity. Some mining outfits produce their own hardware to maximize throughput, but every industrial miner is focused on securing cheap electricity, which is largely influenced by where the operation is located.

Miners geographically concentrate in regions with low-cost electricity. Today, there are mining operations spanning 114 countries globally.[21] According to data collected by Cambridge University, reported mining facilities are mainly located in China, North America, and Europe.[22] Remote areas of China are found to have the highest concentration of mining facilities, as these regions offer low-cost electricity, labor, and equipment. China also boasts numerous ASIC manufacturing plants, underutilized hydropower projects, and an accessible workforce, which represents fertile ground for mining farms. Today, more than half of all mining pools are operated in China.[23,24]

### Figure 7: Geographic dispersion of crypto mining



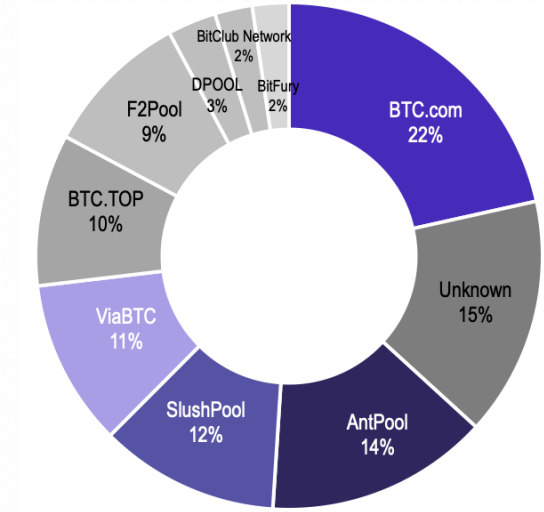

*Source: Dr. Garrick Hileman & Michael Rauchs; University of Cambridge*

21 "Top Five Biggest Crypto Mining Areas: Which Farms Are Pushing Forward the New Gold Rush?" CoinTelegraph (https://cointelegraph.com/news/top-five-biggest-crypto-mining-areas-which-farms-are-pushing-forward-the-new-gold-rush)
22 "Global Cryptocurrency Benchmarking Study," Dr. Garrick Hileman & Michel Rauchs (https://cointelegraph.com/storage/uploads/view/2017-global-cryptocurrency-benchmarking-study.pdf)
23 "Top Five Biggest Crypto Mining Areas: Which Farms Are Pushing Forward the New Gold Rush?" CoinTelegraph (https://cointelegraph.com/news/top-five-biggest-crypto-mining-areas-which-farms-are-pushing-forward-the-new-gold-rush)
24 "Global Cryptocurrency Benchmarking Study," Dr. Garrick Hileman & Michel Rauchs (https://cointelegraph.com/storage/uploads/view/2017-global-cryptocurrency-benchmarking-study.pdf)

## Miner diversity and decentralization

A growing concern for crypto mining is the centralization of hash rate, or the accumulation of mining resources by a small number of individuals and/or entities. Given the high stakes involved, many individuals have chosen to drop solo operation in favor of pools, providing pool operators significant levels of influence. Using bitcoin as an example, a number of established mining pools have come to dominate the market. In fact, of the blocks mined in the last year, over 50% were propagated by the top 4 mining pools, including BTC.com, AntPool, SlushPool, and ViaBTC, as demonstrated in figure 8.[25]

**Figure 8: Top 10 mining pools**




*Source: blockchair.com*

Mining concentration increases the risk of a **51% attack**. Also known as a majority attack, this occurs when a group of malicious validators collude to unilaterally alter transaction history in their favor. However, given the robustness of the mining community for networks like bitcoin, this level of coordination would prove extremely difficult and costly. For other PoW networks with less dedicated mining resources, the cost of establishing a coordinated position may be much lower.[26] One drawback to a 51% attack is the loss of confidence in the integrity of the protocol itself, which may cause the value of the network to plummet. A heavily invested miner would not be able to sustainably attack a network over the long-run, as their attack would result in them accumulating or spending larger amounts of a less valuable (potentially worthless) currency. This disincentive is often cited as a prime deterrent for collusion of mining pools. There has been research to suggest that some of the top mining pools are related, including hardware manufacturers like Bitmain having ownership of BTC.com and AntPool.[27] Theoretically, a heavyweight manufacturer that has vested interest in the top mining pools and manufactures a majority of the hardware used in bitcoin mining could pose a threat to the network. Also, due to the concealed nature of pools, the proportion of hashpower controlled by the pool's mining farms versus individual miners is also unknown. Naturally, this leads to concerns over loss of decentralization and immutability but we believe there is greater incentive for such actors to conduct honest operations and uphold the value of the network.

Furthermore, a balanced Nash equilibrium exists for miners who conduct their operations honestly. A Nash equilibrium is a foundational concept in game theory that refers to a system where participants do not enjoy greater benefits through unilateral action. For crypto miners, block rewards are only credited to participants who build on a valid blockchain that reflects the greater consensus. Any deviation will certainly result in short-term cost with unpredictable compensation. After ten years, Nakamoto consensus has proven to be a robust method for incentivizing honest behavior.

PoS is often cited as an alternative to minimize potential 51% attacks in response to the consolidation of PoW mining. PoS promises individuals better opportunities to act as transaction validators in the network. Instead of purchasing specialized mining equipment, which may be limited or expensive, individuals simply stake their crypto balance for relatively little cost. Under this model, malicious validators can be penalized by forfeiting their stake for attempting to introduce invalid transactions or for attempting to alter transaction history. That said, PoS is not immune to 51% attacks. In theory, a single group capable of acquiring and staking a majority of the supply of a cryptocurrency could choose to alter transaction histories. Here, the implicit cost of diminishing a network's value is the dominant disincentive; colluding parties would have to first acquire the majority of the coin supply, a major cost, and are left holding an enormous bag of losses if users catch on and lose confidence in the protocol itself. If bitcoin were to transition to a PoS validation method, a node or group of nodes would have to amass over $45 billion worth of bitcoin in order to maliciously alter transaction histories.[28]

25 Kraken Intelligence, data obtained from blockchair.com

26 This resource provides an estimate on the theoretical cost of conducting a 51% attack on several number of proof-of-work networks: https://www.crypto51.app/

27 "A look into China's biggest Bitcoin company—Bitmain" Derek Chen (https://medium.com/wolverineblockchain/a-look-into-chinas-biggest-bitcoin-company-bitmain-cf1305eb61c0)

28 Bitcoin market cap is $90 billion as of April 6, 2019 according to blockchain.com

Though the economics and network effects of mining pools favor a consolidated market, low switching costs and equipment mobility prevent sustainable economic moats. This allows new entrants to quickly enter the market and deter oligopolistic collusion. Over time, we expect these market forces to continue to protect the integrity of mining on large crypto networks. Speaking of market forces, let's dive into the economics of mining.

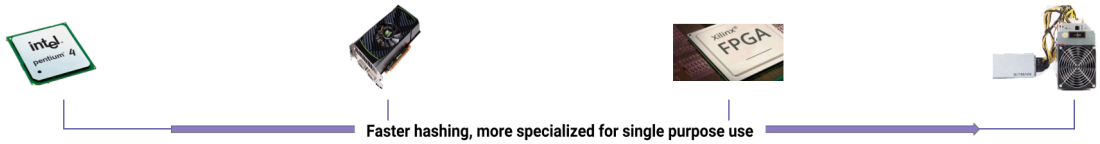
# IV. Economics

The rise of crypto values in 2017 drove a tremendous round of investment in the mining industry. Equipment manufacturers doubled down on R&D to produce the most powerful and efficient ASICs, mining farms fought over locations with access to cheap electricity, and individuals raced to stock up on scarce supplies of performance GPUs. This modern day gold rush exposed the importance of mining economics. In this section, we discuss the evolution of mining equipment, the growth of PoW mining, and a model for examining the profitability of mining on the two largest PoW networks: bitcoin and ethereum.

## Mining equipment

The influx of new miners over the last two years accelerated the era of industrial crypto mining.[29] PoW mining, whose roots begin with bitcoin, has evolved significantly over the last decade. Mining was first conceived by Satoshi Nakamoto as a largely democratic process for transaction validation, where individuals could participate using only their personal computers. Nakamoto referred to this philosophy as "one-CPU-one-vote."[30] Mining with Central Processing Units (CPUs), or processors, would later give way to mining with Graphics Processing Units (GPUs), or graphics cards, and ultimately to Field Programmable Gate Arrays (FPGAs) and Application-Specific Integrated Circuits (ASICs).[31] With each iteration, hardware specialists engineered efficiencies to deliver the most competitive means for hashing new blocks. Figure 9 below summarizes the four epochs of crypto mining, detailing the various trade-offs associated with each advance.

**Figure 9: Crypto mining hardware evolution**




| | 2009<br>Standard multi-core Central Processing Unit<br>**(CPUs)** | 2010<br>Graphics Processing Unit<br>**(GPUs)** | 2011<br>Field Programmable Gate Arrays<br>**(FPGAs)** | 2012<br>Application-Specific Integrated Circuit<br>**(ASICs)** |
|---|---|---|---|---|
| **Function:** | CPU is part of the computer that executes the software installed on the computer. It is highly agile, rapidly switching between tasks and able to follow conditional orders. | GPU is the video rendering system of a computer. It typically assists the CPU with less executive, more repetitive calculations. | FPGAs are customizable chips used to create personal digital circuits. | ASIC is a microchip dedicated to execute hashing algorithms as quickly as possible. |
| **Strengths:** | - Some cryptocurrencies specifically designed for CPUs (restrict participation of more productive hardware types)<br>- No specialized hardware required; CPUs are included in all standard computer systems | - Containing more ALUs than CPUs, able to carry out higher quantity of bulky mathematical orders<br>- No specialized hardware required; installment of special software easily allows mining<br>- Produces less noise | - Faster than both CPU and GPU systems<br>- More electricity efficient per hashing unit, than CPUs and GPUs<br>- Can be re-modified for alternate use as it is not pre-programmed.<br>- Combines the power of an ASIC with flexibility of the GPU | - Most efficient form of hardware as it produces significantly higher hashrate than that of GPUs while requiring a fraction of the power<br>- Easy to use once configured by manufacturer; does not require progamming skills or additional hardware configuration by user |
| **Limitations:** | - Now unprofitable to use for most major cryptocurrencies<br>- Fewer Arithmetic/Logic Units (ALUs) than GPUs, resulting in slower hashing attempts (ALUs are circuits that perform arithmetic operations)<br>- Only supports select cryptocurrencies | - Engineered to run hot, reaching temperatures of 50-70'C under a heavy load<br>- Inefficient as initially designed for gaming and computer graphics, wasted energy and potential when solely used for mining<br>- Requires a computer (motherboards, CPU) to operate | - Scarce and difficult to purchase publicly<br>- Not programmed during roduction; end user must configure each chip, which is challenging for the ordinary crypto miner | - Steep initial investment to purchase hardware<br>- Separate ASIC required for each cryptocurrency coin as it is custom built for single hash algorithms<br>- Generates significant heat and noise, requires ample electricity to run<br>- Cannot be re-modified for alternate use (ie. becomes useless once profitable coins on an algorithm makes a fork)<br>- Existence of ASIC-resistant coins (ie. ethereum) |

*Source: Kraken Intelligence, thenextweb.com(TNW), 1stminingrig.com*

29 "The Evolution of Crypto Mining: Where It Started and Where It's Headed," AMB Crypto (https://ambcrypto.com/the-evolution-of-crypto-mining-where-it-started-and-where-its-headed/)

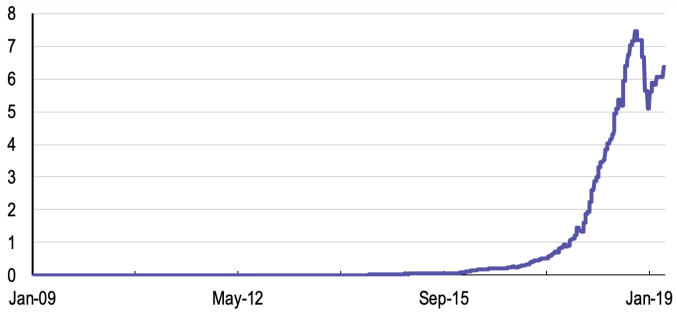
30 "The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote." Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf)

31 "The Evolution of Bitcoin Hardware," Michael Bedford Taylor (https://cseweb.ucsd.edu/~mbtaylor/papers/Taylor_Bitcoin_IEEE_Computer_2017.pdf)

## Growth of PoW Mining

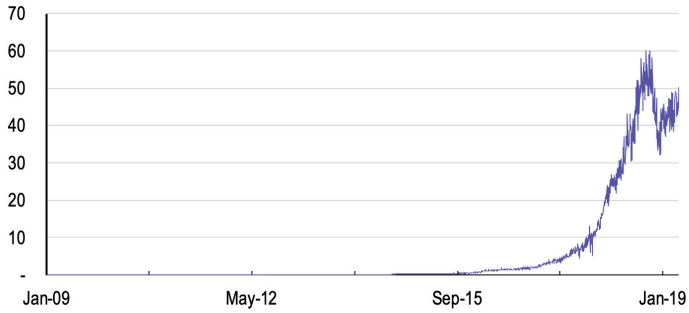
Growth in PoW mining is best measured by the increase in difficulty and **network hash rates** on the bitcoin and ethereum protocols over the last several years. Previously described, PoW mining involves tremendous computational effort to find a valid hash that meets the target difficulty. Using the network's difficulty target, we can infer the network hash rate, or the amount of total computational effort applied to a cryptocurrency protocol at a given time, measured in terahashes per second. For reference, bitcoin's network hash rate clocks roughly 40 etahashes per second, or 40 million terahashes. To appreciate the magnitude of this, 40 etahashes per second is equivalent to guessing and checking 40,000,000,000,000,000,000 hashes every second for a valid block.

**Figure 10: Bitcoin mining difficulty (trillion)**



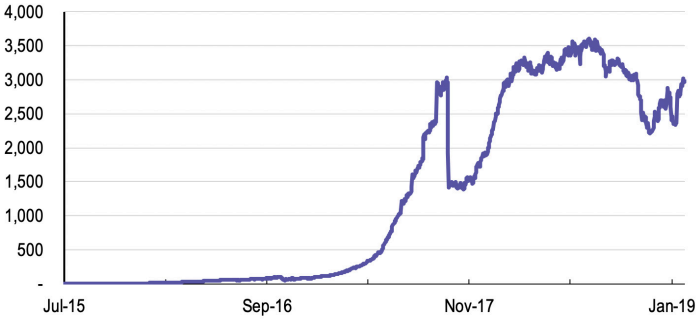

*Source: blockchain.com*

**Figure 11: Bitcoin network hash rate (millions of TH/s)**



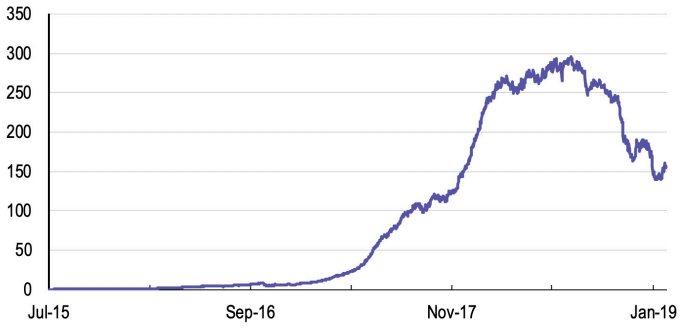

*Source: blockchain.com*

**Figure 12: Ethereum mining difficulty (TH)**




*Source: etherscan.io*

**Figure 13: Ethereum network hash rate (TH/s)**




*Source: etherscan.io*

## Mining profitability

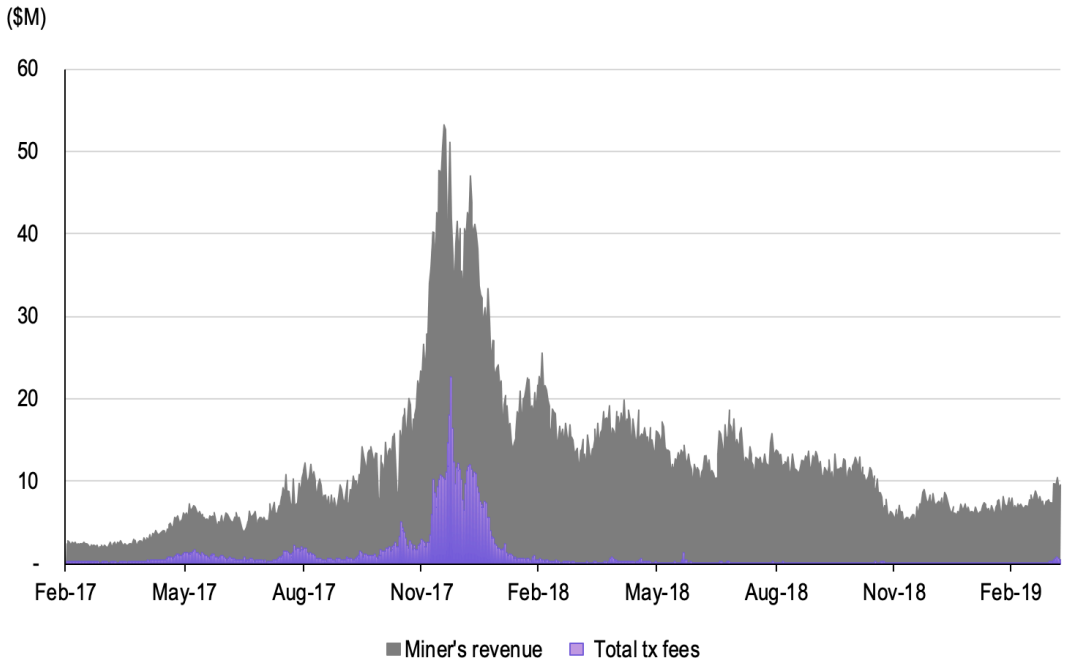
Investing in equipment and infrastructure is not a charitable endeavor. In order for the bitcoin and ethereum blockchains to retain miner support, the networks provide two major incentives: block rewards and transaction fees. Miners continue to mine as long as rewards exceed marginal cost, but before we delve into the P&L, let's first analyze the potential reward.

A block reward is the number of newly minted currency with each new block. Transaction fees represent the collection of all network fees included in a block. Both are credited to the miner who successfully mines a valid block for the network.

Block rewards are intended to function as a subsidy to network validators. Over time, growth in crypto adoption should result in higher transaction fees, which will slowly substitute the need for block rewards in the economic balance. Protocols like bitcoin implement a diminishing rewards schedule, which declines every four years by a rate of 50%. This event is called a **halving**. This schedule is pre-programmed into the protocol and is the reason the supply of bitcoin cannot exceed 21 million bitcoin as designed. Ethereum relies on a different emission schedule, with a static block reward that began at

5 ether per block, declined to 3 ether with Byzantium in late-2017, and recently fell to 2 ether with Constantinople.[32] Over time, ethereum will transition towards a PoS consensus method and is rumored to potentially introduce a coin supply cap at that time. Unique to ethereum, miners also receive rewards for including **ommer blocks (uncle blocks)**.[33] In figure 14, we illustrate that the overwhelming majority of bitcoin mining economics are distributed in the form of block rewards, though transaction fees can be substantial during periods of high congestion.

**Figure 14: Bitcoin miner revenue vs. total tx fees**




*Source: Kraken Intelligence, blockchain.com*

Having understood the rewards, we now turn to the cost of mining. Advances in mining equipment is all about efficiency: how to get the highest and fastest hash rate for the same amount of electricity. The rush of new participants and the rise and dominance of mining pools have made mining major cryptos, like bitcoin, unprofitable for most solo miners. Owing to the computational requirements of PoW, miners seek to optimize for energy and equipment costs.

On the following pages, we model the profitability of mining on the largest PoW networks, bitcoin and ethereum, to measure the P&L of mining in the current environment. Our assumptions are as follows:

+ bitcoin miners employ Bitmain's ASIC Antminer S15, rated at 28TH/s;
+ ethereum miners employ AMD's GPU Radeon RX580, rated at 29MH/s;
+ cost of electricity is $0.04/kWh, the average price of renewable energy;
+ mining equipment depreciates over 2 years of useful life; and
+ the miner is an individual employing a single unit of hardware.

32 Ethereum: A Secure Decentralised Generalised Transaction Ledger - Byzantium Version (https://ethereum.github.io/yellowpaper/paper.pdf)
33 "Orphan, Stale & Uncle Blocks in Bitcoin and Ethereum," Gleb Shirshov (https://2miners.com/blog/orphan-stale-uncle-blocks-in-bitcoin-and-ethereum/)

## Bitcoin economics

Based on the current difficulty of the bitcoin network, access to cheaper electricity would be a prime determinant of profit for miners. Per figure 15 below, we use recent network statistics to measure the P&L of a solo mining operation. This snapshot does not reflect changes in future block rewards, network hash rates, or other variables.

**Figure 15: Bitcoin profitability**

| **BTC** | | Unit |
|---|---|---|
| BTC-USD exchange rate | 5,127 | USD |
| Price of Antminer S15 | 1,020 | USD |
| Hashrate of Antminer S15 (H) | 28,000,000,000,000 | hashes/sec |
| Network hash rate (NH) | 44,809,650,000,000,000,000 | hashes/sec |
| Electricity costs | 0.04 | USD/kWh |
| Equipment power consumption (E) | 1,596 | watts |
| Daily energy consumption by equipment (E*24) | 38,304 | Wh |
| Daily energy expense | 1.5 | USD |
| My share of total BTC network (H÷NH) | 0.00006% | |
| Network total blocks mined a day | 144 | blocks |
| Network total blocks mined a month | 4,320 | blocks |
| Network total tx fee monthly average (1M Avg) | 49 | BTC |
| Block reward | 12.5 | BTC |
| **Revenues and other income** | | |
| Monthly block reward in BTC | 0.03 | BTC |
| **Monthly block reward in USD** | **173.0** | **USD** |
| Monthly tx fee in BTC | 0.00003 | BTC |
| **Monthly tx fee in USD** | **0.16** | **USD** |
| **Total revenues and other income** | **173.2** | **USD** |
| **Costs and other deductions** | | |
| Monthly energy expense (30days) | 44.0 | USD |
| Monthly depreciation expense | 42.5 | USD |
| **Total costs and other deductions** | **86.5** | **USD** |
| EBITDA | 129.1 | USD |
| **Monthly profit (loss)** | **86.6** | **USD** |
| **Straight line depreciation** | | |
| Equipment cost (Antminer S15) | 1,020 | USD |
| Salvage value | - | USD |
| Useful life | 2 | years |
| Monthly depreciation | 42.5 | USD/month |

*Source: Kraken Intelligence, US Energy Information Administration, Bitmain, blockchain.com*
*Note: All network figures as of 7 Apr 2019. Antminer S15 scheduled for release: April 2019.*

## Ethereum economics

Similar to our bitcoin framework, a simplified P&L of a solo mining operation on the ethereum network is presented below as figure 16. In our model, we use a GPU, though there have been developments of Ethash ASIC miners that operate at the high end of the performance scale.

**Figure 16: Ethereum profitability**

| **ETH** | | Unit |
|---|---|---|
| ETH-USD exchange rate | 179 | USD |
| Price of AMD Radeon RX580 | 299 | USD |
| Hash rate of AMD Radeon RX580 (H) | 29,000,000 | hashes/sec |
| Network hash rate (NH) | 145,749,650,500,000 | hashes/sec |
| Electricity costs | 0.04 | USD/kWh |
| Equipment power consumption (E) | 185 | watts |
| Daily energy consumption by equipment (E*24) | 4,440 | Wh |
| Daily energy expenses | 0.2 | USD |
| My share of total ETH network (H÷NH) | 0.00002% | |
| Network total blocks mined a day | 5,760 | blocks |
| Block time | 15 | seconds |
| Seconds in a day | 86,400 | seconds |
| Network total blocks mined a month | 172,800 | blocks |
| Network total tx fee monthly average (1M Avg) | 481 | ETH |
| Block reward | 2 | ETH |
| **Revenues and other income** | | |
| My monthly block reward in ETH | 0.1 | ETH |
| **Monthly block reward in USD** | **12.3** | **USD** |
| My monthly tx fee in ETH | 0.0001 | ETH |
| **My monthly tx fee in USD** | **0.02** | **USD** |
| **Total revenues and other income** | **12.3** | **USD** |
| **Costs and other deductions** | | |
| Monthly energy expense (30days) | 5.1 | USD |
| Monthly depreciation expense | 12.5 | USD |
| **Total costs and other deductions** | **17.6** | **USD** |
| EBITDA | 7.2 | USD |
| **Monthly profit (loss)** | **(5.3)** | **USD** |
| **Straight line depreciation** | | |
| Equipment cost (AMD) | 299 | USD |
| Salvage value | - | USD |
| Useful life | 2 | years |
| Monthly depreciation | 12.5 | USD/month |

*Source: Kraken Intelligence, etherscan.io, US Energy Information Administration, AMD, techradar.com*
*Note: Does not account for change in future block reward, tx fee, and hash rate. All network figures as of 7 Apr 2019.*

To measure the impact of favorable energy rates, we produced sensitivity tables to measure the profitability of mining bitcoin and ethereum assuming different sources of generation and their associated levelized cost of energy, presented as figure 17.

**Figure 17: Sensitivity analysis**

**BTC**

| Source of energy | Cost of energy | Monthly energy expense | Monthly profit (loss) |
|---|---|---|---|
| Hydroelectric | $0.03 | $34.5 | $96.2 |
| Geothermal | $0.04 | $44.0 | $86.6 |
| Solar PV/ Wind, onshore | $0.05 | $56.3 | $74.3 |
| Natural gas | $0.07 | $77.6 | $53.1 |
| Coal | $0.10 | $114.9 | $15.7 |
| Solar thermal/ Wind, offshore | $0.12 | $139.0 | -$8.4 |

**ETH**

| Source of energy | Cost of energy | Monthly energy expense | Monthly profit (loss) |
|---|---|---|---|
| Hydroelectric | $0.03 | $4.0 | -$4.2 |
| Geothermal | $0.04 | $5.1 | -$5.3 |
| Solar PV/ Wind, onshore | $0.05 | $6.5 | -$6.7 |
| Natural gas | $0.07 | $9.0 | -$9.2 |
| Coal | $0.10 | $13.3 | -$13.5 |
| Solar thermal/ Wind, offshore | $0.12 | $16.1 | -$16.3 |

*Source: Kraken Intelligence, US Energy Information Administration (EIA)*

This profitability analysis shows that marginal reward requires better expected frequency of payout and fixed cost absorption. That said, this analysis reflects only a small number of variables and does not factor in the impact of crypto price volatility, changes in difficulty levels, equipment prices, cooling costs, downtime, delivery and customs fees, warehousing and facility costs, accessories, etc.

# V. Externalities

Proof-of-work mining on major cryptocurrency protocols involves an intense, continuous expenditure of electrical energy as machines race to introduce new blocks. This has opened up a major debate on the environmental implications of PoW mining. In this section, we examine the impact of mining on the bitcoin network more closely in an attempt to shed light on the amount of energy required to secure consensus. Determining precise measurements is challenging, so we made the following, simplifying assumptions:

+ miners employ Bitmain's Antminer S9, rated at 14.5TH/s;
+ equipment operates 24/7/365 with no downtime; and
+ hashing is the only form of electricity consumption (excludes factors such as lighting, cooling, etc.)

Of course, miners use a variety of equipment with varying grades of energy efficiency. Given the relatively high efficiency of the Antminer S9, our estimates may underestimate total energy consumption. However, following the decline in crypto-currency values, it's likely that less efficient equipment has been scrapped from service.

**Figure 18: Bitcoin network energy consumption**

| | | |
|---|---|---|
| Hash rate (A) | 44,809,650.0 | TH/s |
| Power efficiency of Antminer S9 (B) | 94.1 | J/TH |
| Total energy consumption / second (A*B) | 4,218,380,451.0 | J |
| **Total energy consumption / year** | 133,030,845,902,736,000.0 | J |
| = | **133,030.8** | **TJ** |
| *(1Wh=3600J)* | 36,953,012,750,760.0 | Wh |
| = | **37.0** | **TWh** |

| **ANTMINER S9 (official specifications for 14.5TH/s batch)** | | |
|---|---|---|
| Energy consumption | 1,365.0 | W |
| Hash Rate | 14.5 | TH/s |
| Power efficiency | 94.1 | J/TH |

| **Energy units** |
|---|
| J= Joules |
| W= Watts |
| TJ= Terajoule |
| TH= Terahash |
| Wh= Watt hour |
| TWh= Terawatt hour |

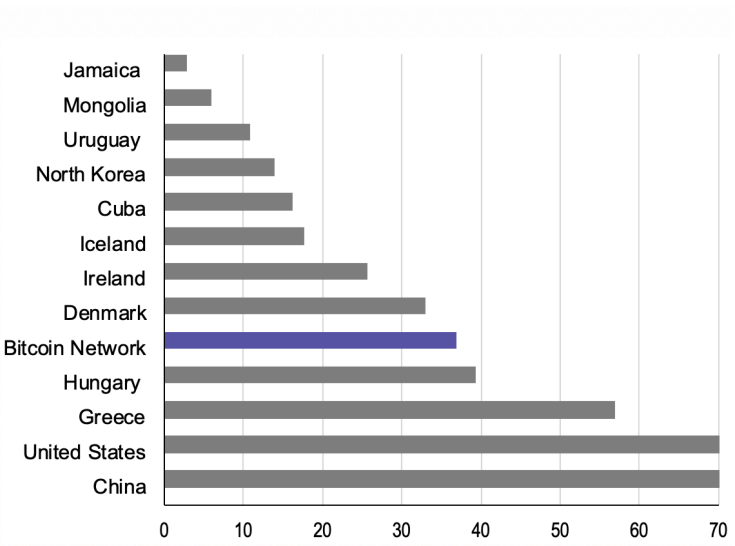
*Source: Kraken Intelligence, Blockchain.com, Bitmain*
*Note: Hash rate as of 7 Apr 2019*

As illustrated in figure 18, bitcoin's network hash rate clocks in around 44 etahashes per second as of April 2019.[34] Using this network hash rate and the Antminer S9's rated power efficiency of 94.1 J/TH[35] we measure bitcoin's total annual energy consumption at roughly 37 terawatt-hours (or 133,031 TJ). This puts bitcoin in rivalry with several industrial countries, as depicted in figure 19.

34 Bitcoin network hash rate provided by blockchain.com (https://www.blockchain.com/charts/hash-rate)
35 Bitmain Antminer S9 technical specifications (https://shop.bitmain.com/promote/antminer_s9i_asic_bitcoin_miner/specification)

**Figure 19: Average annual energy consumption by country**

| Country | Annual energy consumption (TWh) |
|---|---|
| China | 5,564.0 |
| United States | 3,902.0 |
| Greece | 56.9 |
| Hungary | 39.4 |
| **Bitcoin Network** | **37.0** |
| Denmark | 33.0 |
| Ireland | 25.7 |
| Iceland | 17.7 |
| Cuba | 16.2 |
| North Korea | 13.9 |
| Uruguay | 10.8 |
| Mongolia | 5.9 |
| Jamaica | 2.8 |




*Source: Kraken Intelligence, CIA World Factbook*

The bitcoin protocol annually consumes nearly as much energy as Hungary, a nation with 9 to 10 million inhabitants.[36] Media outlets and various reports frequently compare the energy expenditure of the bitcoin network to that of nations as a basis for scrutinizing the ecological sustainability of crypto mining.

Based on our research, the energy footprint of PoW-based cryptocurrencies is highly mobile and tends to follow cheaper, reliable sources of energy. The favored generation source is hydroelectric. For example, many industrial Chinese mining farms that contribute significantly to network hash rate are located in the Sichuan province, where hydropower is an abundant source of energy, produced in surplus quantities.[37] As cheap alternatives become more saturated, cryptocurrency mining may actually spur additional investment in renewable capacity over time.

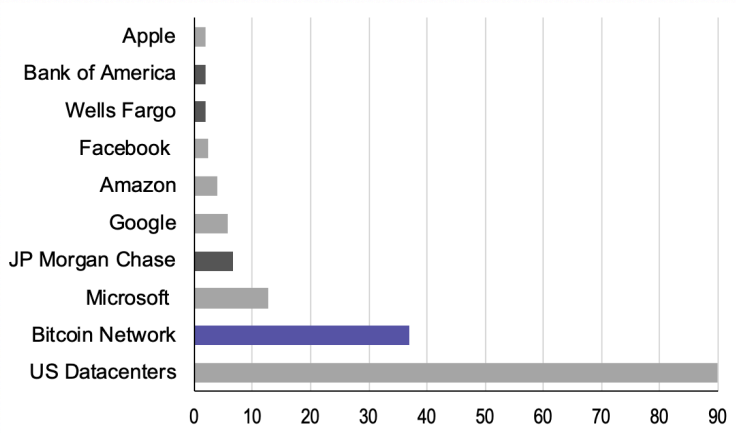
36 World population statistics, The World Bank (https://data.worldbank.org/indicator/SP.POP.TOTL?)

37 "The reports of bitcoin environmental damage are garbage," Robert Sharratt (https://hackernoon.com/the-reports-of-bitcoin-environmental-damage-are-garbage-5a93d32c2d7)

To provide an alternative perspective, we also took a look at the energy consumption of heavy weights in the US tech and financial services industry. Our findings in figure 20 demonstrate that bitcoin mining stacks high relative to individual tech giants like Microsoft, Google, Amazon, Facebook, and Apple, as well as players in the banking industry like JP Morgan, Wells Fargo, and Bank of America. That said, the bitcoin network consumes less than half the load of power hungry US data centers, and only 10% on a global basis. Collectively, it seems that supporting our financial networks, search habits, computing tools, shopping experiences, and social media presence requires almost as much energy as the bitcoin network - a global means of transacting for the 4 billion people with an internet connection![38]

**Figure 20: Annual energy consumption by company**

| Company/data centers | Annual consumption (TWh) |
|---|---|
| Global datacenters | 420.0 |
| US Datacenters | 90.0 |
| **Bitcoin Network** | **37.0** |
| Microsoft | 12.8 |
| JP Morgan Chase | 6.7 |
| Google | 5.7 |
| Amazon | 4.0 |
| Facebook | 2.5 |
| Wells Fargo | 2.0 |
| Bank of America | 2.0 |
| Apple | 1.8 |




*Source: Kraken Intelligence, Statista, techspot.com, Forbes, data-economy.com, AWS, JPM, BoA, WFC*
*Note: consumption is based on 2017 with the exception of JPM (2016) and Google (2015). JPM denotes US consumption levels while BoA and Wells Fargo denote global consumption levels.*

In an age where conservation efforts are critical, it's difficult to favorably debate the importance of a robust mining network. But this 37TWh of energy consumption represents a fortress with respect to the security of the bitcoin protocol. Imagine the dedicated effort required to alter the transaction ledger - a collection of individuals and entities with enough equipment and generation capacity - larger than entire nations - to even have a chance. As cryptocurrency continues to see more adoption over time, we anticipate the utility value of blockchain technology to outweigh the societal costs, particularly with respect to mining.

38 Global internet usage statistics, International Telecommunications Union (ITU) (https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx)

# VI. Summary & Conclusion

Mining has come a long way since the days of Satoshi and one-CPU-one-vote. Nowadays, warehouses full of whirring machines expend massive amounts of computational effort to validate transactions for large crypto protocols.

In this note, we described blocks as little more than collections of transaction data, shared in a public ledger - the block-chain. We detailed the process of PoW mining and noted the rise of PoS consensus methods, including the trade-offs from a security and network accessibility standpoint.

After a brief introduction of the key equipment manufacturers, we bifurcated miners into two groups: solo and pool miners. In particular, we noted that the competitive intensity has pressured many miners today to contribute their hashing efforts to large syndicates, mining pools, which propagate the largest share of blocks on the bitcoin protocol. This consolidation of mining resources has led to growing concerns of majority attacks. However, we discussed an underlying game theory of PoW to show that consensus follows Nash equilibrium such that majority attacks are not in the best interest of adversarial participants. In addition, we noted the rise of PoS as an alternative consensus method to minimize potential attacks.

This consolidation has taken place over several years of advances in equipment efficiencies. The rise in difficulty rates has driven commercial operations to optimize for costs, particularly with respect to sourcing cheap electricity. Despite the global span of mining operations, most mining takes place in China, North America, and parts of Europe, largely in regions with abundant hydroelectric capacity. This digital gold rush towards commercial scale operations has displaced the partic-ipation of casual, solo miners, who struggle to profitably mine on the bitcoin and ethereum network without similar access to cheap electricity.

We commented on the bitter reality that securing these protocols isn't cheap and PoW networks, specifically, consume a lot of energy. We estimated that the bitcoin protocol consumes as much electricity as a small country, but disagreed with the perspective that the network energy consumption is wasteful, as a network is only as safe as the cost to attack it.

As adoption grows and blockchain technology matures, we believe it's important for crypto users to have a greater ap-preciation for mining and its foundational purpose in transaction validation. We hope this introductory-level explanation equips you with an understanding of the core concepts and the role of mining in decentralized networks. Despite the vari-ous perspectives that color this industry, the topic of mining is undergoing significant study - from consensus algorithms to sources of energy consumption - and we hope this note brings clarity to an otherwise complex topic and encourages you to engage in further discussion.

# Glossary

**51% attack (majority attack):** a coordinated effort to alter transaction histories by securing more than 50% of validating authority.
+ Proof-of-work networks are vulnerable when a group of colluding miners control a majority of network hash rate.
+ Proof-of-stake networks are vulnerable when a group of colluding stakers control a majority of staked coin supply.

**Airdrop:** a cryptocurrency distribution method that allows holders of a different crypto protocol to claim and/or spend the airdropped currency. Airdrops are designed to quickly increase the number of potential network participants.

**Blockchain fork:** a divergence in software versions that can result in multiple transaction histories through a blockchain split.
+ **Hard fork:** protocol changes that are not backward-compatible with older versions of software, requiring all nodes to update their clients. Miners and nodes may abandon the older state of the blockchain, thereby resulting in no additional chain states. In a contentious fork, multiple factions operate both old and new versions of software, which results in divergent transaction histories.
+ **Soft fork:** backward-compatible protocol changes that follow both old and new consensus rules and do not result in a chain split.

**Block:** a collection of transaction data and other blockchain metadata.

**Blockchain:** a distributed public ledger that contains a complete record of all previous transactions. Blocks contain metadata that reference predecessor blocks, forming a chain structure. Attempts to alter a single link (block) on the chain will invalidate the remainder of the chain and will be rejected by the broader network of consensus nodes.

**Block header hash:** the hashed output of a block's input string. Each block has a unique block header hash.

**Block height:** the total number of valid blocks included on a blockchain. Each block increases the height by 1.

**Block reward:** newly minted coin supply awarded to miners for a successfully mined block.

**Block time:** the expected amount of time required to introduce a new, valid block.

**Block timestamp:** the timestamp of a block indicated in seconds elapsed in UNIX time (since 1 January 1970).

**Coinbase:** the first transaction included in every block that provides miners with a reward of newly minted coin supply.

**Confirmation:** a recognition that a transaction has been included in a block, which consensus nodes have accepted as valid. Transactions included in a valid block on the main chain are said to be "confirmed." The number of confirmations represents the number of successive blocks that have been added to the chain since a transaction was first confirmed.

**Difficulty target:** a hexadecimal number that begins with a consecutive number of zeros ("leading zeros"). A miner's goal is to successfully validate a block by producing a hash that meets the minimum level of difficulty, considered a valid proof-of-work.

**Double spend:** spending the same unit of currency twice by altering transaction history to invalidate the first recorded spent transaction. This is analogous to using the same check for two different transactions, knowing one of the transactions will bounce.

**Ethash:** a cryptographic hash function utilized by the ethereum protocol.

**Forging (minting):** the validation process for introducing new blocks on a proof-of-stake network. Functionally equivalent to mining.

**Genesis block:** the first valid block recorded on a blockchain.

**Halving:** also known as a block reward halving, this is a periodic reduction in block rewards. On the bitcoin protocol, this periodic reduction amounts to 50%.

**Hash:** a string, or a series of numbers and letters, often fixed in length. This is the output of a hashing function.

**Hexadecimal number**: a base-16 numerical system where 0 - 9 represent values zero to nine and A - F represent values ten to fifteen. A hash is often represented as a hexadecimal number.

**Initial Coin Offering (ICO)**: a crowdfunding campaign seeking to raise cryptocurrency funds to build an application or product.

**Main chain:** a chain of blocks recognized by the majority of consensus nodes as the valid record of transaction history.

**Mempool:** a collection of broadcasted, unconfirmed transactions waiting to be included in a block. Also known as a "memory pool."

**Merkle root:** a hash of a block's merkle tree.

**Merkle tree:** a binary tree-like structure for efficient storage, where transactions in a block are hashed together recursively using SHA-256 until the process results in one final hash: the merkle root.

**Mining:** the validation process for introducing new blocks on a proof-of-work network. Functionally equivalent to forging.

**Mining pool:** a coordinated group of individual miners sharing computational resources to increase the group's chance of successfully validating a block.

**Nakamoto consensus:** a consensus rule utilized by the bitcoin protocol that recognizes the chain with the most accumulated proof-of-work (longest chain) as the main chain.

**Network hash rate:** a measure of the computational resources engaged in proof-of-work mining on a cryptocurrency protocol. This metric represents the number of hashes generated per second by miners actively seeking to introduce a valid block.

**Nodes:** servers on a cryptocurrency network that maintain transaction records and broadcast newly introduced information.
+ **Full nodes:** nodes that store the full blockchain and transaction history of a protocol.
+ **Lightweight nodes:** nodes that store only block headers and rely on a full node's copy of the blockchain to broadcast or verify whether a transaction has been validated.

**Nonce:** an arbitrary number that is used once and then incremented, or adjusted by 1, after each attempt by a miner to produce a valid hash.

**Orphan block:** a block that meets the minimum required proof-of-work, determined by the difficulty target, but is not included in the main chain because it does not have a recognized parent block.

**Ommer blocks (uncle blocks):** stale blocks on the ethereum protocol that are not orphaned and can be "re-included" later in the main chain by a miner for a reward. This is useful for blockchains where blocks are introduced more frequently, and thus susceptible to higher orphan rates.

**Previous block hash:** the block header hash of a preceding block in the main chain.

**Secure Hash Algorithm-256 (SHA-256):** a cryptographic hash function, utilized by bitcoin and other cryptocurrency protocols, which yields a unique 256-bit output (hash) regardless of the length of the input.

**Share difficulty:** difficulty levels established by mining pools, below network difficulty targets, in order to distribute mining reward pro rata among participants in the pool.

**Solo miner:** miners that operate individually rather than in collaboration with others in a pooled effort.

**Stale block:** a block that meets the minimum required proof-of-work, determined by the difficulty target, but is no longer included in the main chain due to a competing branch achieving consensus.

**Transaction fees:** the sum of all network fees from transactions included in a block, credited to the miner if they successfully introduce a valid block to the network. Also directly referred to as "network fees" or "miner tips."

**Version number:** the software version of a cryptocurrency protocol, which is often included in block metadata to allow participants to track the adoption of upgrades and which consensus rules to follow on a protocol.