ARK INVEST

Bitcoin Mining

The Evolution of A Multibillion Dollar Industry

Published: 9 March, 2020

Author: Yassine Elmandjra,
Blockchain and Cryptoassets Analyst at ARK Invest

Co-Author: Derek Hsue,
Investments and Research Team Member at Blockchain Capital

CONTENTS

I.	**Introduction**	3
II.	**The Importance of Proof of Work**	3
	Is Proof-of-Work Inefficient?	4
	The Cost to Reverse a Transaction	5
III.	**The Role of Hardware**	7
	The Evolution of Bitcoin Miner Hardware	7
	The Rise of ASIC Commoditization	9
	Manufacturing and Distribution	11
	Sizing the Miner Hardware Opportunity	11
IV.	**The Operations of Mining**	12
	The Evolution of Mining as an Operation	12
	Manufacturers and Self-Mining	13
	The Cost to Mine	13
	The Geography of Mining	14
	The State of Mining Pools	15
V.	**Miner Influence**	20
	Do Miners Set the Price Floor?	20
	Are Miners Whales?	21
	Addressing Mining Attack Vectors	22
VI.	**The Future of Bitcoin Mining**	24

I. Introduction

Bitcoin's innovation lies in its ability to coordinate trust and facilitate the transfer of value without relying on a centralized authority. The enabler is proof-of-work mining, a mechanism that adds new bitcoin to the money supply and protects the network against nefarious actors' attempting to spend the same bitcoin more than once. Through economic incentives, miners voluntarily secure the network by verifying "blocks" of transactions and appending them to Bitcoin's public ledger. Specialized, dedicated hardware perform a function that proves that a miner has executed a costly computation. In exchange for providing the processing power that is critical to the network's security, miners are rewarded with newly minted bitcoin and transaction fees.

As of this writing, Bitcoin's network value, or market capitalization, is roughly $150 billion,[1] with bitcoin mining one of the most significant beneficiaries of its appreciation during the last 10 years. Once dominated by hobbyists drawing central processing units (CPU) from desktops, mining has evolved into a hyper-competitive, multibillion-dollar industry[2] harnessing specialized chip hardware.

While it is essential to the security of Bitcoin, ARK believes mining is both opaque and misunderstood. As Bitcoin continues to gain economic stature, investors and users must investigate and understand the very industry that contributes to securing the network. This paper aims to analyze the supply chain associated with the mining industry, from hardware to manufacturing and operations, and to highlight the implications on Bitcoin's future.

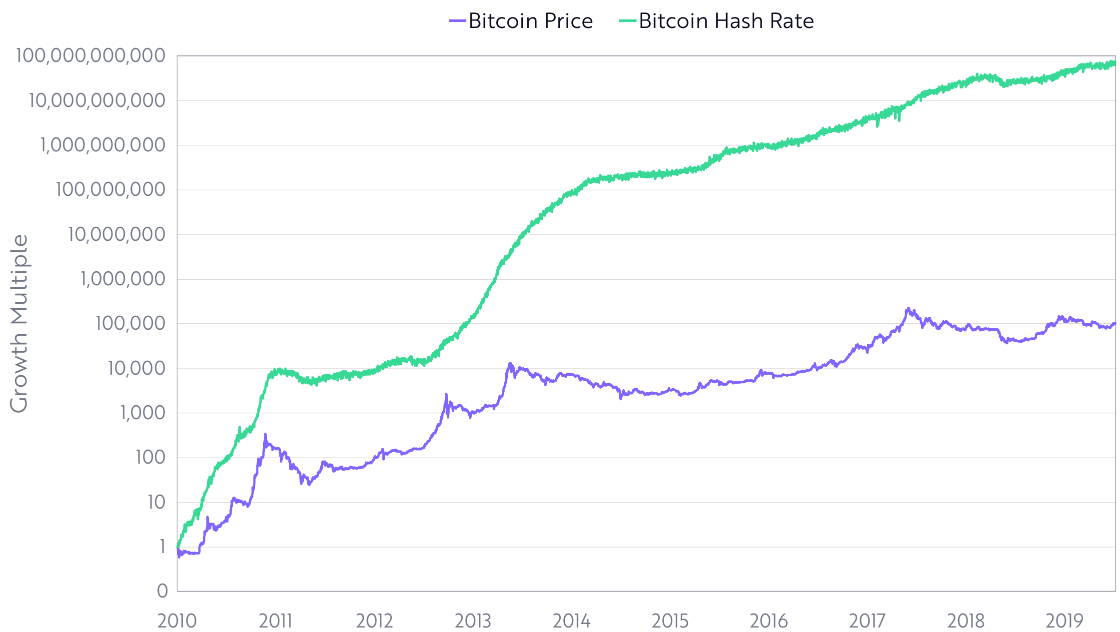
II. The Importance of Proof-of-Work

Proof-of-work mining (PoW) is critical to achieving consensus without a central trusted authority. In the Bitcoin network, trustworthiness is protected by computation. As entities compete to solve computationally intensive mathematical problems based on a cryptographic hash algorithm, they provide proof of execution of a costly computation. A hash algorithm inputs arbitrary data and outputs a deterministic string of fixed length. The process of hashing a "block" of transactions repeatedly until it matches a target output is known as mining. The only way miners can solve the mathematical problem, or produce a hash matching the target, is by performing the operation repeatedly until the solution is found by chance. The likelihood of a miner finding the solution increases in proportion to the resources it expends.

1 *Cryptocurrency Market Capitalizations." CoinMarketCap, coinmarketcap.com/.*
2 *"Mining." Mining - Bitcoin Wiki, en.bitcoin.it/wiki/Mining.*

Today, solving the problem - "proof" that a miner has executed a costly computation - requires quintillions of hashing operations per second. As shown in the graph below, hashrate has increased by roughly an order of magnitude every year for the last 6 years and at a rate 4 times faster than the appreciation in bitcoin's price during the last 5 years, a function of hardware technology advances and miners' expectations of the rise in bitcoin's price. As of March 1 2020, Bitcoin's hash rate was at all time highs, standing at 136 quintillion hashes per second, as shown below.

Figure 1: Bitcoin Price vs. Hash Rate Growth



Source: ARK Investment Managvement LLC, 2020; Data Sourced from: coinmetrics.io

Is Proof-of-Work Inefficient?

Proof-of-work critics often assert that the process consumes significantly more resources than it creates. What critics deem computationally inefficient and unscalable, however, advocates consider not only an intended tradeoff but a fundamental feature.

As highlighted by founder of Bit Gold and Bitcoin pioneer Nick Szabo,[3] "Prolific resource consumption and poor computational scalability unlock the security necessary for independent, seamlessly global, and automated integrity." ARK believes Bitcoin has a unique ability to provide powerful settlement assurances in a trust-minimized manner because specialized, dedicated hardware perform a function that proves the computer has executed a costly computation.

3 *"Money, Blockchains, and Social Scalability." Money, Blockchains, and Social Scalability | Satoshi Nakamoto Institute, nakamotoinstitute.org/money-blockchains-and-social-scalability/.*

Bitcoin makes the tradeoff explicit: by allocating significant real-world resources to mining, Bitcoin guarantees settlement[4] like no other network. In The Anatomy of Proof Work,[5] Chaincode Labs resident Hugo Nguyen explains that "under the hood, proof-of-work mining converts kinetic energy (electricity) into a ledger block. By attaching energy to a block, one gives it 'form', allowing it to have real weight and consequences in the physical world."

Additionally, we believe that Bitcoin's electricity expenditure is orders of magnitude less than the electricity expenditure of alternative banking and monetary systems. According to Dan Held, Head of Business Development at Kraken,[6] the banking system uses 2.4 billion gigajoules (GJ) annually, the gold mining industry 500 million GJ, while Bitcoin uses a fraction of the two, at 184 million GJ annually. Contrary to consensus thinking, we believe the environmental impact of bitcoin mining should also be di minimis. Renewables are estimated to account for 77.6% of total bitcoin mining.[7] In their search for the cheapest form of electricity, miners are likely to continue flocking to regions offering a glut of renewable electricity, unlocking stranded energy assets as "electricity buyer[s] of last resort, creating a highly mobile base-demand for any electricity sources able to produce at prices below current producers, regardless of location."

The Cost to Reverse a Transaction

A Bitcoin transaction cannot be reversed without rewriting the history of transactions that took place after that transaction, an energy intensive exercise that has become prohibitively expensive. Even though transactions are not "final" or "absolutely" immutable, the deeper they are buried in the ledger, the more economically irrational it becomes to reverse them. As a result, Bitcoin derives its immutability from the prohibitive cost to rewrite or append transactions, which in turn is a function of the network's cumulative proof-of-work.

As shown in Figure 2, the cumulative work performed on the Bitcoin network exceeds 10^{27} hashes. In other words, to rewrite Bitcoin's transactions history would require more than 10^{27} computations, and to rewrite just 6 blocks of its history would require 300 trillion computations.

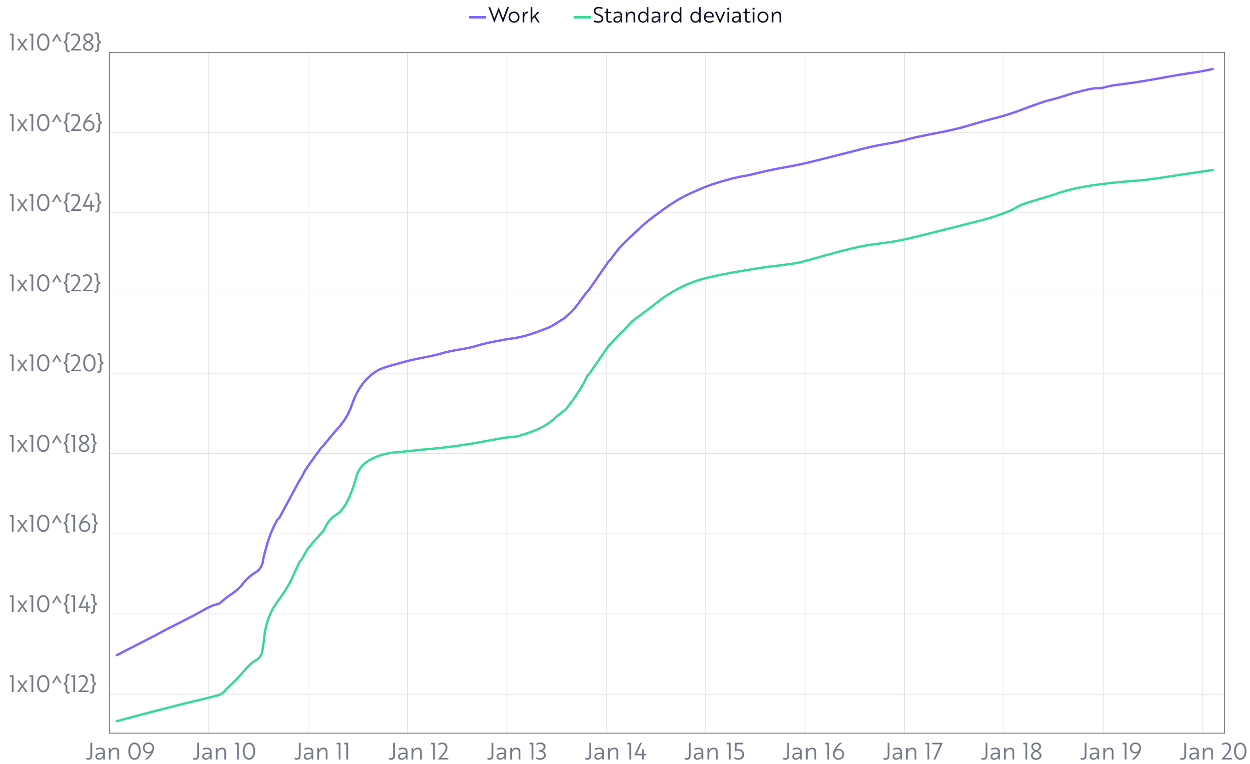
4 *Carter, Nic. "It's the Settlement Assurances, Stupid." Medium, Medium, 5 Aug. 2019, medium.com/@nic__carter/its-the-settlement-assurances-stupid-5dcd1c3f4e41.*

5 *Nguyen, Hugo. "The Anatomy of Proof-of-Work." Medium, Bitcoin Tech Talk, 3 Jan. 2019, bitcointechtalk.com/the-anatomy-of-proof-of-work-98c85b6f6667.*

6 *Held, Dan. "PoW Is Efficient." Medium, Medium, 11 Aug. 2019, medium.com/@danhedl/pow-is-efficient-aa3d442754d3.*

7 *"The Bitcoin Mining Network: Trends, Marginal Creation Costs, Electricity Consumption & Sources." Https://Coinsharesgroup.com/Research/Bitcoin-Mining-Network-November-2018, CoinShares, Nov. 2018.*

Figure 2: Bitcoin network total computations



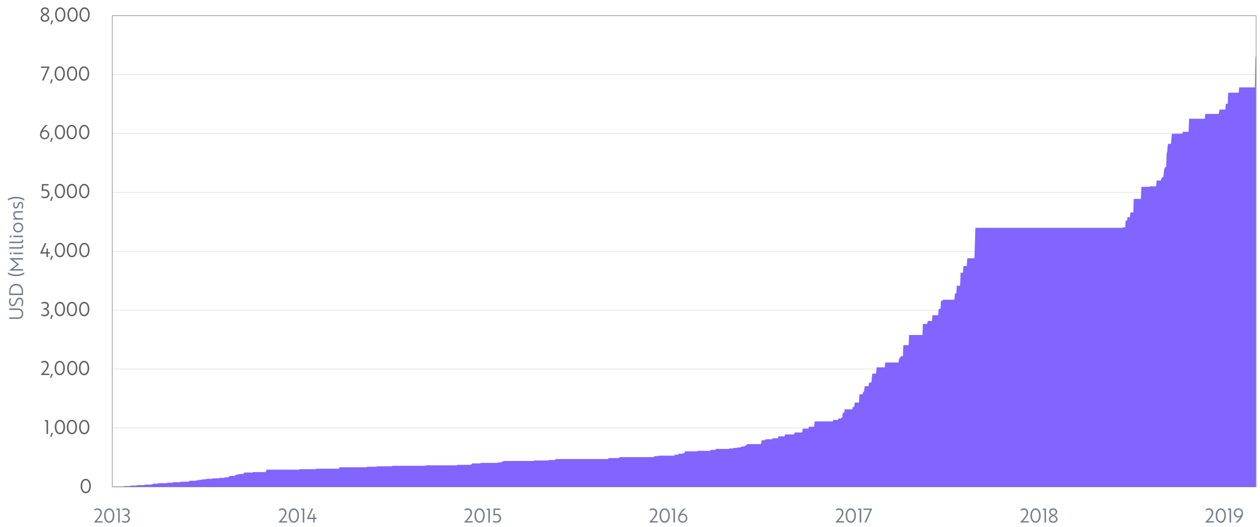
Source: http://bitcoin.sipa.be/work-ever.png

Typically, to secure a transaction, the recipient should wait until the cost to reverse it is higher than the value of the transaction itself.[8] Today, an hour's worth of computational power on the Bitcoin network costs nearly $1 million,[9] suggesting that the eight or more hours necessary to rewrite a single block would be prohibitively expensive.[10]

The barriers to rewriting transactions go well beyond the cost of the computational power. Miners must also purchase hardware dedicated to mining bitcoin. According to our estimates, 8 million units of the most cost-efficient mining hardware would be necessary to support current hashrate activity: at $500 on average per mining unit, the cost to duplicate the installed base today would be $4 billion. Since 2013, we estimate all of the hardware put in place to support Bitcoin's cumulative hashrate has cost $7.2 billion, as shown in Figure 3.

8 *For instance, if a transaction is worth $10 million, the recipient should wait approximately 10 hours before providing the good or service.*
9 *"PoW 51% Attack Cost." Crypto51, www.crypto51.app/.*
10 *Bloomberg.com, Bloomberg, www.bloomberg.com/opinion/articles/2019-01-16/bitcoin-and-other-cryptocurrencies-are-open-about-being-at-risk#footnote-1.*

Figure 3: Estimated Cumulative Miner Hardware Cost



Source: ARK Investment Management LLC, 2020

III. The Role of Hardware

Solving the proof-of-work algorithm profitably requires running specialized hardware, the sole purpose of which is mining bitcoin. Since the inception of dedicated Bitcoin hardware in 2013, we believe billions of dollars have been spent on design, production, and tapeout, spawning an industry dedicated exclusively to manufacturing this robust and specialized hardware. In the next section, we analyze the evolution of miner hardware and its supply chain.

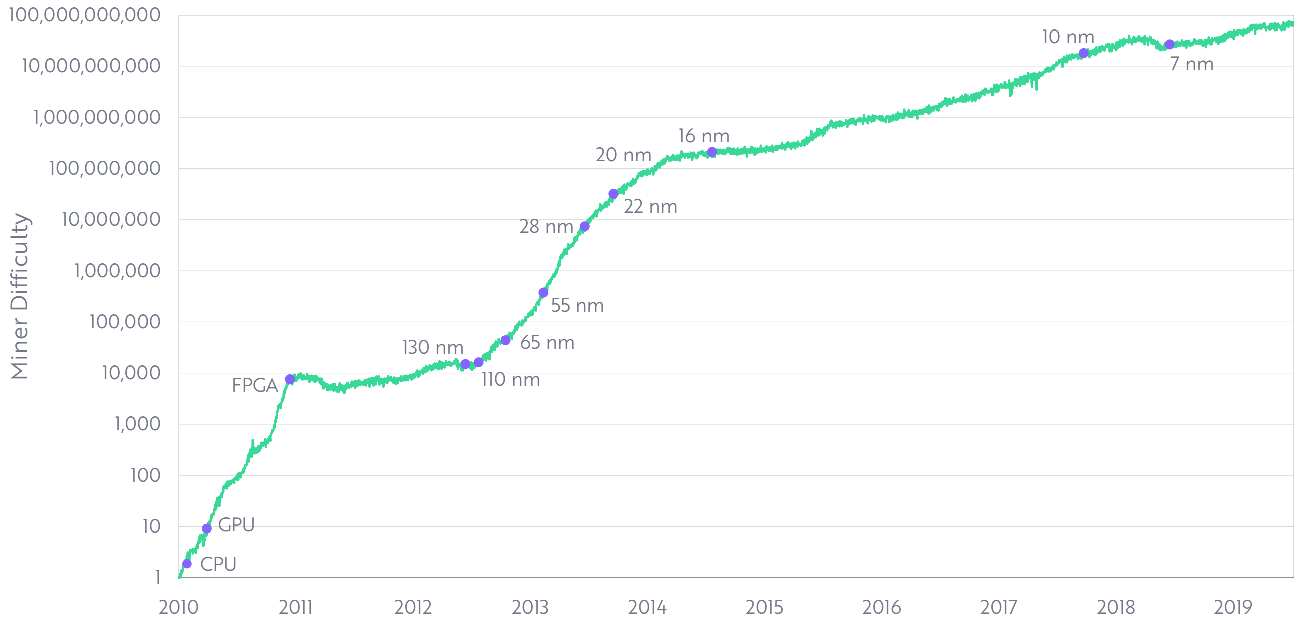
The Evolution of Bitcoin Miner Hardware

In 2009, Bitcoin mining began as a hobbyist activity. The first miners performed computations on desktops with standard central processing units (CPUs). About a year later, the first publicly available miner equipped with graphics processing unit (GPU) surfaced. With the introduction of GPUs, the computational difficulty increased rapidly, hurting the profitability of mining on traditional desktops. In response, pooled mining enabled consortia to mine collectively, splitting the rewards pro rata. In mid-2011, developers demanded even more specialized hardware equipped with field-programmable gate arrays (FPGA).

Today, we believe the most efficient Bitcoin hardware is powered by application specific integrated circuits (ASICs), chips designed specifically for mining bitcoin. In 2013, the launch of Bitcoin ASICs spurred professionalization of the mining industry, placing most of the computational power in specialized data centers.

The difficulty of mining increased as the hardware evolved, pointing to a correlation between hardware efficiency gains and the difficulty to mine, as shown below.

Figure 4: Hardware Evolution vs. Miner Difficulty



Source: ARK Investment Management LLC, 2020; Alliance Bernsetin

Taiwan Semiconductor Manufacturing Company (TSMC), Samsung, and Intel are the only foundries[11] today working on cutting-edge semiconductor nodes.[12] Only TSMC and Samsung, however, are relevant to Bitcoin mining, suggesting that innovation in the space is somewhat hostage to a duopoly. Because these foundries allocate capacity that is scarce at the high-end and because miner efficiency is a function of process nodes, the relationship between mining equipment manufacturers and foundries is crucial to their success.[13]

Moreover, the switching costs from one foundry to another appear exceptionally high, as their production processes are finely tuned and vary. Switching is rare because the cost often includes the complete redesign of an ASIC.[14]

We believe that as the capital necessary to fabricate leading edge nodes mounts, the likelihood of new competitors entering the space will diminish. As hash power decentralizes, chip fabrication will likely remain concentrated.

11 *"Semiconductor Device Fabrication." Wikipedia, Wikimedia Foundation, 20 Feb. 2020, en.wikipedia.org/wiki/Semiconductor_device_fabrication.*

12 *This is not a recommendation in relation to any named securities and no warranty or guarantee is provided. Any references to particular securities are for illustrative purposes only.*

13 *Other supplier relationships and components may be multi-sourced and easily replaced, such as the controller functions or component suppliers providing MOSFET power transistors. TSMC is the world's largest foundry and captures greater than 50% of the world's market share. At the advanced nodes, we believe they unequivocally lead the charge and consistently outperform industry averages. Bitmain, for instance, uses TSMC's 12, 16, and 28 nm process nodes and has announced its transition to 7nm for their next nodes.*

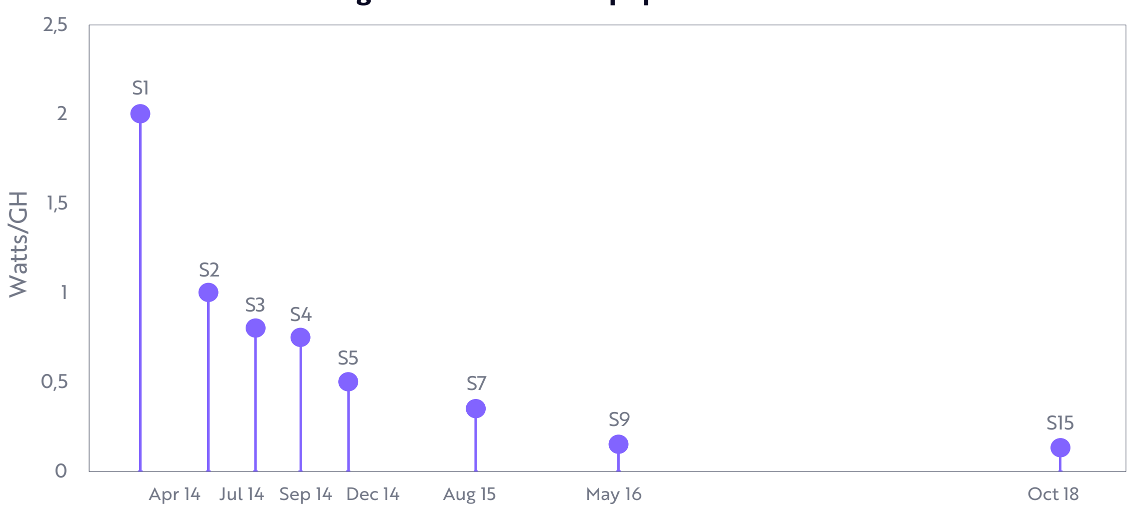
14 *Theoretically, a miner manufacturer could become dissatisfied over time and engage with another foundry for future nodes, but we believe even that is unlikely. Engagements with foundry partners are likely to last at least a few years, with engagement on a single node basis lasting 12 - 18 months.*

The Rise of ASIC Commoditization

Over the last 5 years, Bitcoin ASIC replacement cycles have lengthened significantly. In the early days, they were short, with designs obsolete within months.[15] In November 2013, the largest mining machine manufacturer, Bitmain, shipped its first batch of 55 nm Bitmain S1s running at 2,000 Watts/Terahash (W/TH). The following summer, it released[16] its 28 nm S3 which, at 773.8 W/TH, was nearly 3 times more efficient than its predecessor.

Now that the Bitcoin ASIC design space has caught up to Moore's Law,[17] however, the design cycle has slowed down significantly. As shown in Figure 5, Bitmain has labored to advance its Antminer at the same rate as in the past.

Figure 5: Antminer Equipment Release Dates



Source: ARK Investment Management LLC, 2020; Data Sourced from bitmain.com

In the past, Bitmain could iterate rapidly because mining was behind the latest node technology curve. In 2015, its S7 was the cutting edge ASIC mining chip at 28 nm technology, for example, but Intel had been shipping more advanced 14 nm nodes to consumers in 2014.[18] During the next few years, Bitmain's design cycles continued to lengthen primarily because of bottlenecks at the foundry level and management turnover at the ASIC design level.[19] We believe that competition from other mining hardware manufacturers also has increased dramatically. Two years ago,

15 *Taylor, Michael Bedford. The Evolution of Bitcoin Hardware. THE IEEE COMPUTER SOCIETY, 2017, cseweb.ucsd.edu/~mbtaylor/papers/Taylor_Bitcoin_IEEE_Computer_2017.pdf.*

16 *Hajdarbegovic, Nermin. "Bitmain Releases Energy Efficient 478GH/s AntMiner S3." CoinDesk, CoinDesk, 30 June 2014, www.coindesk.com/bitmain-releases-energy-efficient-478ghs-antminer-s3.*

17 *Moore's Law: Gordon Moore's prediction that the number of transistors on a chip would double every two years.*

18 *"14 Nm Process." Wikipedia, Wikimedia Foundation, 1 Feb. 2020, en.wikipedia.org/wiki/14_nm_process.*

19 *Bitmain becoming the leading miner manufacturer from 2013-2017 and struggling thereafter exemplifies the importance of the ASIC design team to a manufacturer's success. Bitmain's dominance evolved in large part due to the quality of the Antminer S7 and S9 machines. The performance of the S9, driven by its efficient design, allowed Bitmain to rapidly gain market share and become the largest manufacturer. Three years after release, the S9 is still one of the most popular Bitcoin miners until very recently. Upon designing the S9, Yang Zuoxing, a former director responsible for the Antminer designs, left Bitmain to start a competing manufacturer - Bitewei. With Yang at the helm, Bitewei released the Whatsminer M10, a mining rig considerably more efficient than the S9. During this same time, Bitmain was rumored to have struggled with its 10nm and 7nm designs, in part due to the departure of Yang.*

Bitmain's Antminer S9 was the industry leader, 3 times more powerful than the industry average. Today, it has no competitive edge, as shown in the two graphs below.

Figure 6: 2016 vs 2019 Antminer S9 Competition

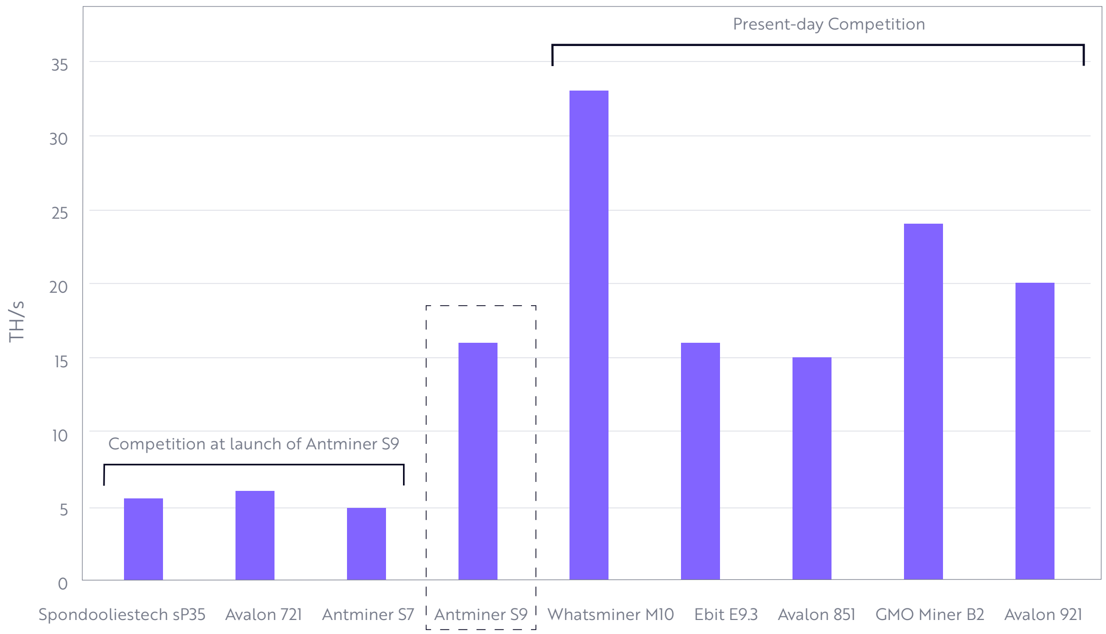
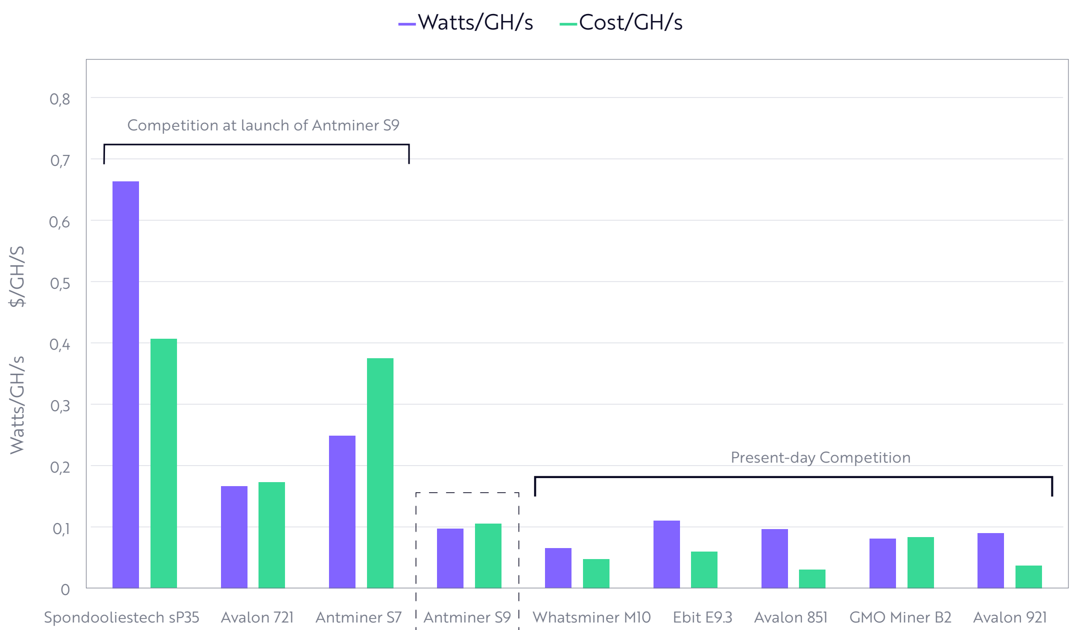


Figure 7: 2016 vs 2019 Antminer S9 Competition Efficiency Metrics



Source: ARK Investment Management LLC, 2020; Data Sourced from bitmain.com

Compared to the few months it took Bitmain to launch a next generation miner a few years ago, present day cycles allow for plenty of time for competitors to get to market. Several original equipment manufacturers (OEMs) have entered the Bitcoin ASIC industry, including Innosilicon, Canaan, and Whatsminer. Canaan, the industry's second largest manufacturer, recently filed for an IPO.[20]

Manufacturing and Distribution

Key to success in manufacturing mining hardware is optimizing the packaging reliably and efficiently. With proprietary processes in packaging and systems integration, mining chip manufacturers can lower the thermal density of their ASICs, increasing performance and lowering costs.[21]

ASIC hardware manufacturing involves the following steps. The manufacturers:

1. Receive wafers from the foundry.
2. Test the wafers for fabrication errors with prediction models.[22]
3. Test and package the wafers within an integrated circuit (IC) design.[23]
4. Ship the ICs to printed circuit board (PCB) manufacturers for mounting.
5. Integrate the completed boards with other electronic components to create the final product.

Mining machine companies believe that their manufacturing processes will differentiate them, delivering competitive advantages. Canaan's IPO prospectus states, "Through a unique combination of applying silicon in the construction, customized packaging and system integration, the thermal density of our proprietary ASICs can be made lower."[24] These improvements are small, however, suggest that any edge in efficiency and power consumption will be commoditized as competition evolves.

Sizing the Miner Hardware Opportunity

Based on our research, the mining hardware industry will be valued at a fraction of the ecosystem it is creating. If Bitcoin's network value were to appreciate roughly 7-fold from $150 billion to $1 trillion during the next 5 years, for example, the mining equipment industry might approach a $20 billion valuation. At today's bitcoin network value, its fair value probably is less than $5 billion.

20 *"Bitmain Competitor Canaan Publicly Files for $400M IPO on Nasdaq." The Block, www.theblockcrypto.com/linked/44963/bitmain-competitor-canaan-publicly-files-for-ipo-on-nasdaq.*
21 *New Listing Information - AP & PHIP, www1.hkexnews.hk/app/appindex.html.*
22 *This process is known as "scan testing" and uses a pre-determined suite of signals that tests each gate on the chip. The tested wafers are sewn into individual dies.*
23 *This consists of custom packaging for the die. The packaging team must optimize for signal integrity, thermal efficiency, reliability, and cost. This step is highly customizable and a potential point of differentiation across firms. For example, early Bitmain machines were known for their superior thermal design. It is common for firms to outsource certain parts of the packaging and testing process - though they vary in how much they do in-house vs outsourced. For example, Canaan relies on a number of production partners, including ChipPAC, SPIL, and STATS ChipPAC for IC packaging and testing.*
24 *New Listing Information - AP & PHIP, www1.hkexnews.hk/app/appindex.html.*

If Bitcoin were to reach $1 trillion in network value, miners probably would generate roughly $15 billion in annual revenue from block rewards and transaction fees consistent with a 2024 inflation schedule and a transaction fee to market cap ratio of 1%. Given a two year hardware replacement cycle, depreciation would consume 50% of their revenue per year, suggesting that miners would not be willing to pay more than $7.5 billion for equipment annually.

While the largest mining machine manufacturers have reported[25] EBITDA margins higher than 50%, their margins are likely to settle at or near the 30% for traditional semiconductor and equipment manufacturers,[26] yielding an industry EBITDA of $2.25 billion. If the equity market were to value them at 10 times EBITDA, the total Enterprise Value attributable to mining equipment manufacturers would be roughly $20 billion. Consequently, discounting to today's $150 billion in Bitcoin network value, the total enterprise value attributable to mining equipment companies should not exceed $5 billion.[27]

IV. The Operations of Mining

The Evolution of Mining as an Operation

As the industry has professionalized, mining operations have changed substantially. Mining data centers are now industrial-scale facilities with management and servicing on par with traditional cloud data centers.[28] Contracts often are long term and built for multiple hardware cycles requiring significant upfront capital spending and power supplies ranging in the hundreds of megawatts. Electricity is a critical consideration in the economics of mining facilities, with low-cost stranded renewables particularly attractive.[29] Miners have also begun to leverage vented and flared natural gas at upstream oil and gas facilities.[30] Additionally, governments are offering electricity subsidies to attract miners who will set up operations and steer their countries toward the leading edge of innovation.[31]

25 *Zhao, Wolfie, and Stan Higgins. "Bitcoin Mining Giant Bitmain Just Officially Filed for an IPO." CoinDesk, CoinDesk, 27 Sept. 2018, www.coindesk.com/bitcoin-mining-giant-bitmain-files-ipo-prospectus-in-hong-kong.*

26 *"Margins by Sector (US)." Operating and Net Margins, pages.stern.nyu.edu/~adamodar/New_Home_Page/datafile/margin.html.*

27 *For context, Bitmain's most recent proposed valuation was $12 billion.*

28 *Kampl, Alex. Analysis of Large-Scale Bitcoin Mining Operations (or How Bitcoin Miners Make $845 Million a Year). Allied Control, 2014, www.allied-control.com/publications/Analysis_of_Large-Scale_Bitcoin_Mining_Operations.pdf.*

29 *Bendiksen, Christopher. "Beware of Lazy Research: Let's Talk Electricity Waste & How Bitcoin Mining Can Power A Renewable…" Medium, CoinShares, 1 Nov. 2019, medium.com/coinshares/beware-of-lazy-research-c828c900b7d5.*

30 *"Bitcoin Mining: Upstream Data Inc.: Lloydminster, Alberta." Upstream Data, www.upstreamdata.ca/.*

31 *Alderman, Liz. "Despite Bitcoin's Dive, a Former Soviet Republic Is Still Betting Big on It." The New York Times, The New York Times, 22 Jan. 2019, www.nytimes.com/2019/01/22/business/georgia-bitcoin-blockchain-bitfury.html.*

Manufacturers and Self-Mining

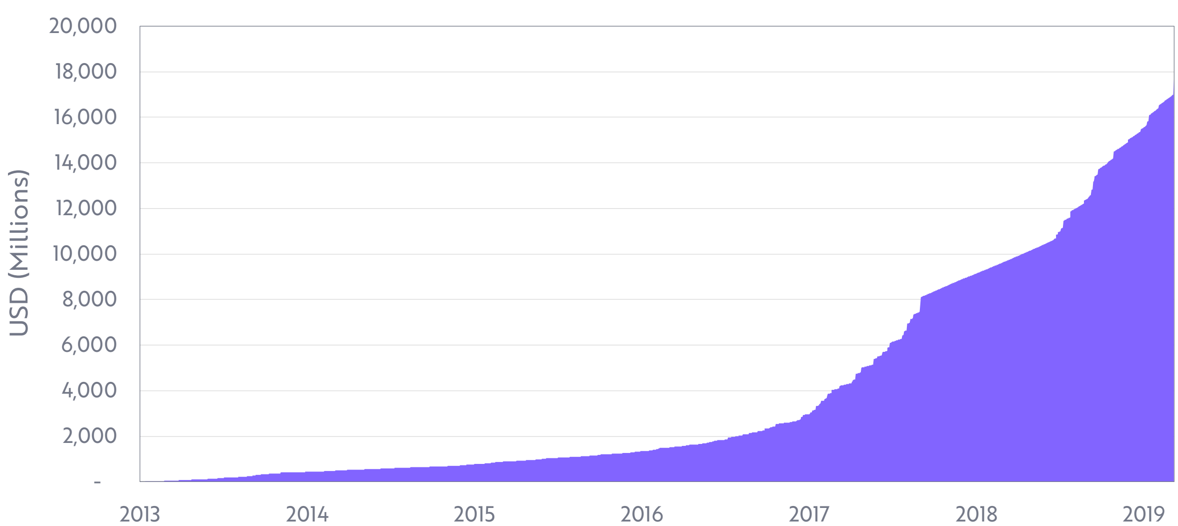
In the past, mining machine manufacturers have tried to leverage their own hardware by opening up mining facilities. Not only are they able to deploy hardware at the cost of goods sold but they also can control the delivery of hardware to competing miners, which begs the question of why they would sell any hardware in the first place?

As Obelisk founder David Vorick has stated in the past,[32] "A well-funded profit maximizing entity is only going to sell a money printing machine for more money than [it expects...to] get from printing it." We believe that among the reasons mining machine manufacturers would sell hardware are the following. The expertise to operate mining facilities is very different from that to manufacture hardware, much like manufacturing oil drilling equipment requires competencies different from those in oil exploration and development. Manufacturing is a capital-intensive process with significant lead times. Moreover, without a competitive advantage in sourcing electricity, mining machine manufacturers could be uncompetitive despite their hardware cost advantages.

The Cost to Mine

Profitability levels for miners vary across operations. Given their highly competitive nature, large-scale Bitcoin miners tend to operate privately. Their capital spending is largely a function of hardware, and their operating expenses a function of electricity, cooling, and maintenance. According to our research, based on Bitcoin's historical hashrate and the advances in mining hardware since 2013, miners have spent $17.6 billion to deploy, operate, and support their expansion, as shown below.[33]

Figure 8: Estimated Cumulative Mining Costs Incurred



Source: ARK Investment Management LLC, 2020

32 *Vorick, David. "The State of Cryptocurrency Mining." Medium, Sia Blog, 14 May 2018, blog.sia.tech/the-state-of-cryptocurrency-mining-538004a37f9b.*
33 *Our estimation for the total cost of mining is driven by several assumptions. At a high level, the mining cost components we incorporate into the model include electricity, hardware, maintenance/cooling, leasing, and expansion costs.*

To illustrate the cost to mine bitcoin, assume a miner has purchased hardware with a hashing rate of 16 TH/s for $750. When in service, the hardware consumes 1 kilowatt of electricity costing 5 cents per kilowatt hour and incurs maintenance, leasing, and cooling costs of 3 cents per kilowatt hour. In total, running the hardware for a year would cost $700. At current Bitcoin difficulty, the miner is expected to generate approximately .1 bitcoin annually. Extrapolating the costs to mine a full bitcoin (assuming a 12.5 bitcoin block reward) comes out to ~$7000 per bitcoin plus the cost of hardware. At 3 cents per kilowatt hour of electricity cost, the cost to mine a bitcoin is roughly $5000.

The Geography of Mining

A number of factors can influence hardware and electricity costs. Historically, most large mining farms have set up their operations in China for a number of reasons, some of which have diminished in importance. Among them are the following:

To leverage local infrastructure and scale rapidly

- Given one- to six-month hardware replacement cycles in the early days of mining, farms had to hit the ground running to generate positive returns on investment in a business that might be profitable for just a few weeks to months. Based on shorter deployment times, shipping, and overhead costs, China was a logical location because Asian foundries supply most of the chips for mining hardware. Now that design cycles are lengthening, however, we believe the competitive dynamics are shifting from geographical proximity and rapid deployment to product reliability and energy costs.

To take advantage of cheap electricity in sweetheart deals with municipalities

- Historically, Chinese miners cut deals with power-plant owners and local municipalities to access cheap electricity. Mining farms proliferated in Sichuan, for example, attracted by the access to cheap electricity from its hydroelectric power stations.[34] With a surplus in hydro-power capacity, Sichuan wanted to capitalize on what otherwise would have been stranded assets. Now that the Chinese government has turned hostile toward cryptoassets and ramped up pressure on miners,[35] the political risk is rendering mining untenable. Local governments also are hurting the economics with new taxes as well as regulations on the price of electricity and the use of land.

As China forces them out, mining operations are diversifying geographically with the cost of electricity a primary consideration. Many countries offer competitive electricity rates, including Iceland, Canada, and the US.[36]

34 *Hileman, Dr. Garrick, and Michael Rauchs. Global Cryptocurrency Benchmark Study. Cambridge Centre for Alternative Finance, 2017, www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf.*

35 *Deng, Chao. "China Quietly Orders Closing of Bitcoin Mining Operations." The Wall Street Journal, Dow Jones & Company, 11 Jan. 2018, www.wsj.com/articles/china-quietly-orders-closing-of-bitcoin-mining-operations-1515594021.*

36 *Alderman, Liz. "Despite Bitcoin's Dive, a Former Soviet Republic Is Still Betting Big on It." The New York Times, The New York Times, 22 Jan. 2019, www.nytimes.com/2019/01/22/business/georgia-bitcoin-blockchain-bitfury.html.*

Chinese mining machine manufacturers also are beginning to hedge against an intensified crackdown by the Chinese government. As Canaan states in its IPO filing, "An increasing portion of [its] revenues has been derived from sales to customers outside the PRC - changes in policies and laws regarding holding, using, or mining of bitcoins could result in an adverse effect on [its] business operations."[37]

The State of Mining Pools

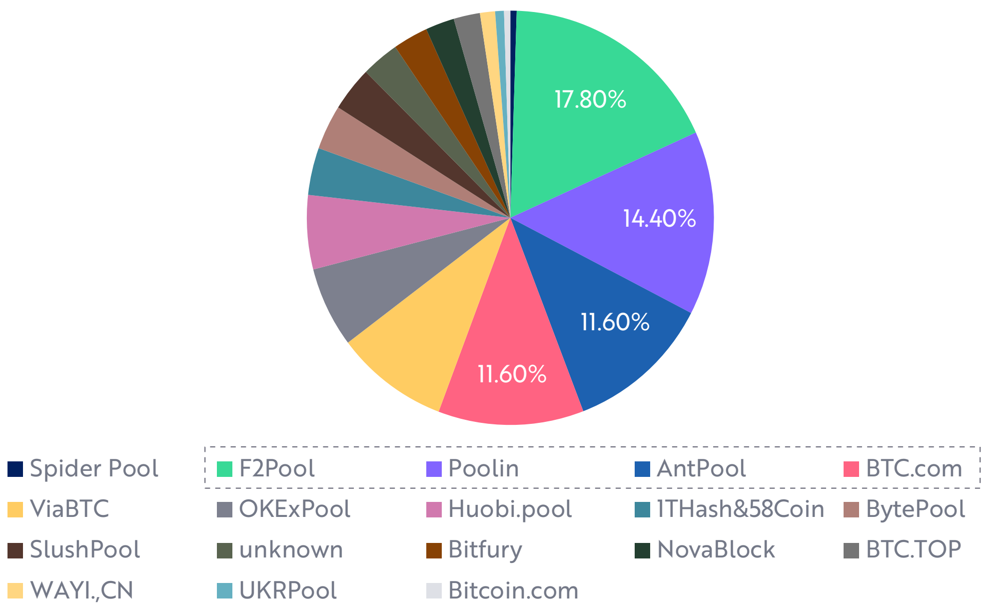
Mining pools were introduced in late 2010[38] in response to the increased proof-of-work difficulty inhibiting individual miners from consistently mining blocks. A traditional CPU miner today would need centuries to mine a block. By pooling resources and sharing processing power in mining pools, small-scale operations can survive on more predictable and timely payouts.

Bitcoin critics often cite mining centralization as a notable risk to the security of the network. Because individuals no longer can mine profitably, hashrate does seem to have consolidated into a handful of mining pool operators, though many critics conflate entities running mining pools with entities that own and operate their own mining equipment. While Bitmain owns and operates a small percentage of global hashrate,[39] it also manages two mining pools with mining equipment owned and operated by third parties. Miners are free to come and go as they please. Fearing centralization, they can switch to different pools, as has historically been the case.[40]

As shown in the Figure 9, the current hashrate distribution among mining pools is somewhat concentrated. The top four mining pools account for more than 51% of Bitcoin's hashrate. Notably, Bitmain not only operates both AntPool and BTC.com but also owns a stake in ViaBTC.

37 *New Listing Information - AP & PHIP, www1.hkexnews.hk/app/appindex.html.*
38 *"Pooled Mining." Pooled Mining - Bitcoin Wiki, en.bitcoin.it/wiki/Pooled_mining.*
39 *New Listing Information - AP & PHIP, www1.hkexnews.hk/app/appindex.html. Self-mining accounts for just 5-10% of Bitmain's revenue.*
40 *Hajdarbegovic, Nermin. "Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack." CoinDesk, CoinDesk, 15 Apr. 2014, www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack.*

Figure 9: Hashrate Distribution by Mining Pool



Source: ARK Investment Management LLC, 2020; Data Sourced from: btc.com

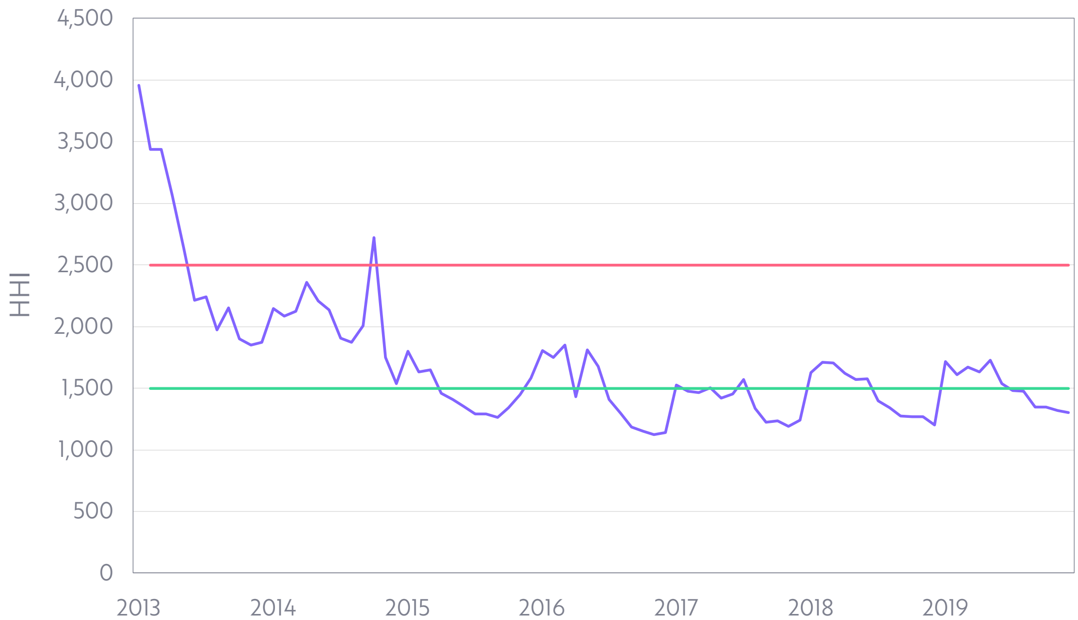
We have assessed the level of mining pool centralization with the Herfindahl-Hirschman Index (HHI), a common heuristic for determining market concentration.[41] "The U.S. Department of Justice considers a market with an HHI of less than 1,500 to be a competitive marketplace, an HHI of 1,500 to 2,500 to be a moderately concentrated marketplace, and an HHI of 2,500 or greater to be a highly concentrated marketplace."[42]

According to three versions of the HHI, the mining industry is surprisingly competitive. In the first version, "Unknown" is a single entity. As shown in Figure 10, the HHI for mining pools has improved over time, with the only instance of concentration in 2013. Since then, the HHI has declined on average in every year and currently stands at 1,300.

41 *The HHI is calculated by squaring the market share of each firm competing in the market and then summing the resulting numbers. For example, for a market consisting of four firms with shares of 30, 30, 20, and 20 percent, the HHI is 2,600 (302 + 302 + 202 + 202 = 2,600)*

42 *Hayes, Adam. "Why the Herfindahl-Hirschman Index (HHI) Matters." Investopedia, Investopedia, 11 Feb. 2020, www.investopedia.com/terms/h/hhi.asp.*

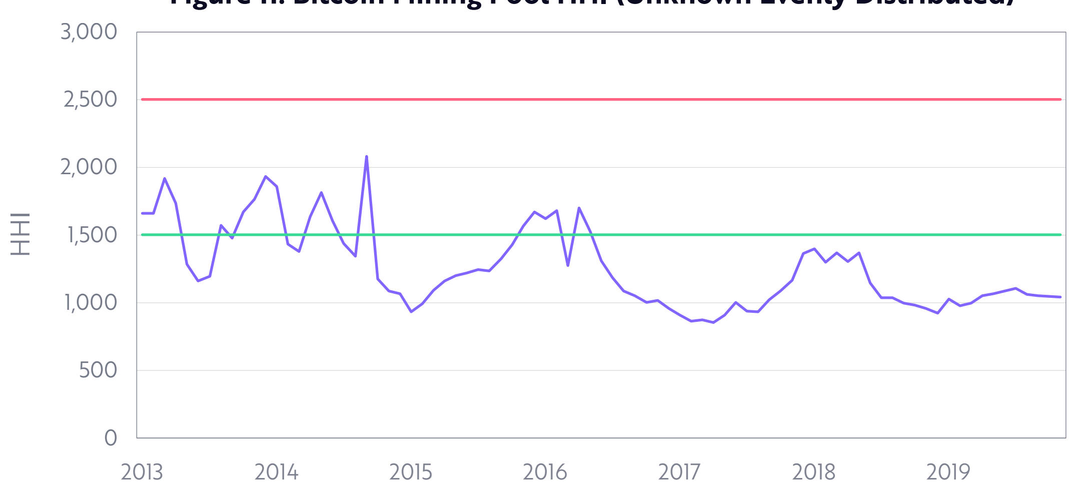
Figure 10: Bitcoin Mining Pool HHI Pool



Source: ARK Investment Management LLC, 2020; Data Sourced from: btc.com

More realistically, "Unknown" is comprised of several mining pools. In the graph below, the HHI assumes that "Unknown" consists of 15 evenly distributed mining pools. In this context, the mining pool industry has never been a "concentrated marketplace". Since 2013, this version of the HHI has hovered between 700 and 1,700, averaging 1,228.

Figure 11: Bitcoin Mining Pool HHI (Unknown Evenly Distributed)



Source: ARK Investment Management LLC, 2020; Data Sourced from: btc.com

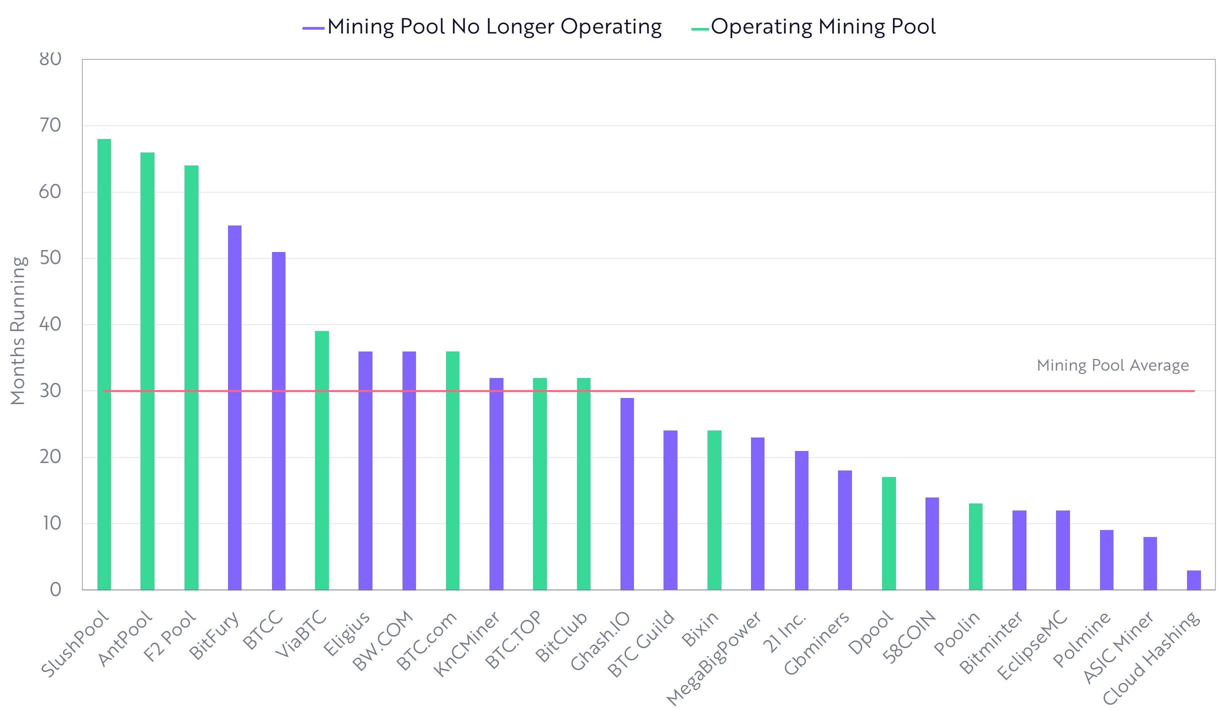
We also calculated a version of the HHI that accounts for Bitmain's influence over BTC.com, F2Pool, and 50% of ViaBtc, so much so that they are considered a single entity. Under this assumption, the HHI peaked in 2018 at ~2050, has declined since, and suggests that the mining pool industry currently is competitive.

Bitcoin critics claim that Bitmain, as a single entity, is the most powerful player in the space, able to dictate Bitcoin's future at the mining pool level. Based on the HHI, even when consolidating the mining pools associated with Bitmain into one entity, the industry is competitive.

Another way to assess the state of mining pools is by turnover in the competition, as measured by the average lifetime of mining pool operators. Because the HHI measures only the current state of the mining pool ecosystem, it does not account for turnover. In "centralized" industries, turnover typically is low. In a competitive industry, no player remains dominant indefinitely. In that context, the chart below is illuminating.

In the last 5 years, the average mining pool's lifetime has been 2.5 years. Of the 26 mining pools in operation 5 years ago, 16 are defunct. The longest running mining pool, SlushPool, has controlled approximately 6% of Bitcoin's hashrate over its lifetime. Furthermore, dominant mining pools do not maintain their leads over time. The largest mining pools during the industry's short life - BTC Guild and Ghash.io – once controlled as much as 20% of the hashrate but no longer exist, as shown in Firgure 12 and 13.

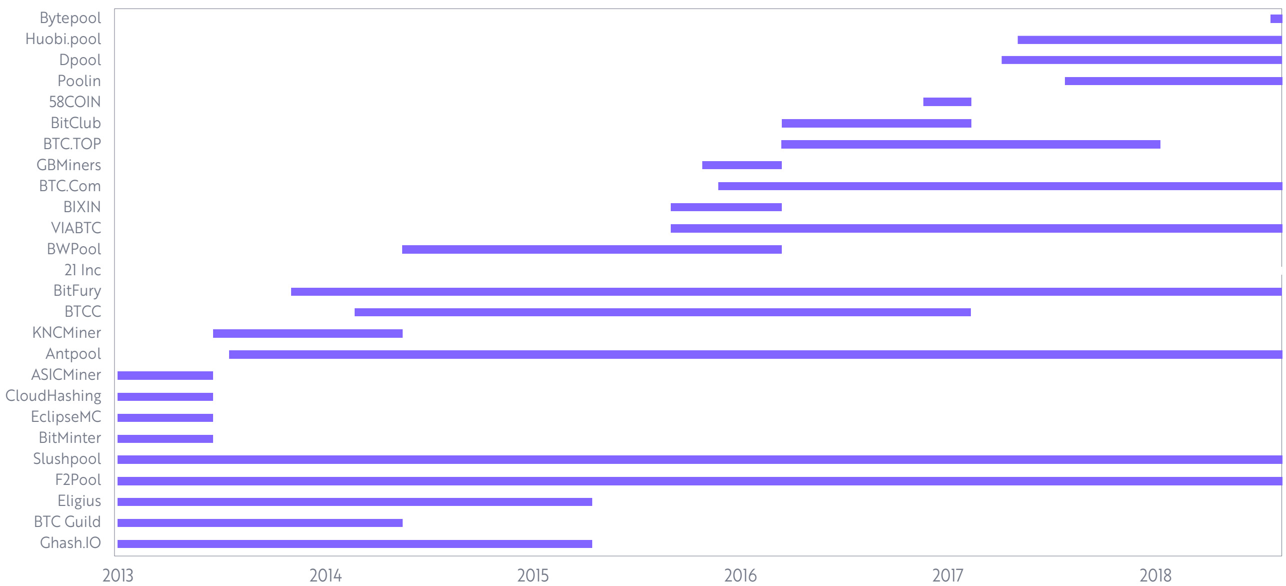
Figure 12: Mining Pool Turnover



Source: ARK Investment Management LLC, 2020; Data Sourced from: btc.com

In the last 5 years, the average mining pool's lifetime has been 2.5 years. Of the 26 mining pools in operation 5 years ago, 16 are defunct. The longest running mining pool, SlushPool, has controlled approximately 6% of Bitcoin's hashrate over its lifetime. Furthermore, dominant mining pools do not maintain their leads over time.

Figure 13: Bitcoin Mining Pools' Length of Time in Top 10



Source: ARK Investment Management LLC, 2020; Data Sourced from: btc.com

While we believe mining pools are competitive today, efforts like the BetterHash protocol to distribute hashpower further are imperative. Even if mining pool operators do not control the hashrate themselves, they run the node, construct the block, select the transactions, and choose what fork will receive their miners' hashpower.[43] With enough hashpower, mining pool operators could exert censorship control over the network.[44] To guard against that possibility, in August 2019 Bitcoin technology company Blockstream announced[45] Blockstream Pool, the first production mining pool based on the BetterHash protocol.

43 *Decrypt, Stop and. "BetterHash: Decentralizing Bitcoin Mining With New Hashing Protocols." Crypto Words Now WORDS, 12 July 2019, cryptowords.github.io/betterhash-decentralizing-bitcoin-mining-with-new-hashing-protocols.*

44 *The Stratum Protocol is the current standard adopted by mining pool operators. As explained by core developer Matt Corallo, "the design of the Stratum protocol requires pool operators to build and distribute block templates to their clients. Without a diverse body of miners constructing block templates, the network's censorship resistance is jeopardized (e.g. pool operators may use their position of power to restrict the flow of protocol upgrades)."In March of 2018, Matt Corallo released the BetterHash Mining Protocol. With the Stratum protocol, miners can actually «steal» hashpower from the pool operator by pretending to be that operator. BetterHash has a far more effective authentication mechanism. In BetterHash, block construction and payouts would be divided into two protocols, Work and Pool. Instead of mining pool operators, individual miners would have discretion over which transactions to include in the blocks, while still benefiting from a stable payout. By controlling block templates, individual miners are no longer exposed to the risk of mining pools censoring transactions.*

45 *Cook, Chris, and Samson Mow. "Announcing Blockstream Mining and Pool." Blockstream, 8 Aug. 2019, blockstream.com/2019/08/08/en-mining-launch/.*

V. Miner Influence

The impact miners have on the Bitcoin network is a hotly debated topic. Does hashrate drive price? Can the value of a bitcoin be linked to the costs of producing it? Are miners whales? What are the threats to mining? We explore some of these questions below.

Do Miners Set the Price Floor?
Production costs have been hypothesized as a link to fundamental valuations. Termed the labor theory of value,[46] the hypothesis is that "the value of a commodity can be objectively measured by the labor hours and energy required to produce that commodity." Prevalent in the 18th and 19th centuries, its proponents argue that the labor theory can value all commodities, with prices in excess of that 'fundamental valuation' as the profits.

Applying this theory, researchers can derive the average production price per bitcoin after accounting for capital spending (capex) and operating expenses (opex). With data from bitcoin miners, they can calculate the mean cost of production and a uniform production price.

This commodity pricing framework, however, fails to incorporate bitcoin's supply schedule. Typical exploration and development companies respond to price signals and vary production accordingly, while bitcoin's issuance is mathematically metered and does not vary.

If the price of a traditional commodity like gold increases, companies will increase production until the marginal cost equals the market price minus transport costs. If the price falls, production will drop until the marginal cost equals the market price. Relative to what otherwise would be the case, volatility drops as supply increases in rising price markets and supply decreases in falling price markets.

In contrast, bitcoin's issuance is predefined, its supply curve inelastic, suggesting that bitcoin miners cannot set a price floor. Regardless of the amount of mining resources, the difficulty adjustment forces the issuance of bitcoin to be consistent over time.[47] If miners enter or exit the ecosystem, difficulty adjusts accordingly to stabilize the rate of issuance. If the cost of production rises, unprofitable miners may simply exit the system. This characteristic sets bitcoin apart from all other commodities and along with its fixed supply, determines its volatility. While they might serve as a gauge of miner profits and margins, we believe production costs are unlikely to be the primary determinant of bitcoin's price.

46 *"Labor Theory of Value." Wikipedia, Wikimedia Foundation, 21 Feb. 2020, en.wikipedia.org/wiki/Labor_theory_of_value.*
47 *Bendiksen, Christopher. "An Honest Explanation of Price, Hashrate & Bitcoin Mining Network Dynamics." Medium, CoinShares, 27 Sept. 2019, medium.com/coinshares/an-honest-explanation-of-price-hashrate-bitcoin-mining-network-dynamics-f820d6218bdf.*

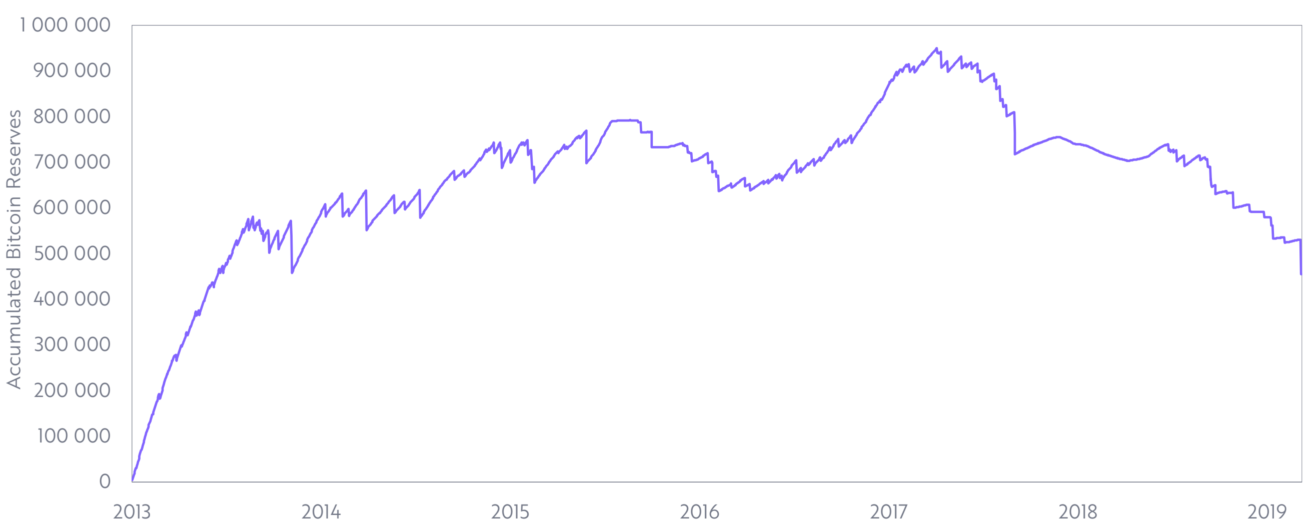
Are Miners Whales?

Mining is the only process through which bitcoin is issued and distributed, at least initially. In other words, miners have had first claim to every bitcoin in circulation today, suggesting that they could have had significant control over the market if they never sold any of their rewards. Since the professional bitcoin mining industry evolved in 2013, debates have surfaced and intensified over its impact on and control of market conditions.

Miner reserves are controlled theoretically on the upside by the sum of newly issued supply and transaction fees. Since December 2013, miners have generated nearly 6 million bitcoin (BTC) in revenue, or USD $42.6 billion which, all else equal, would account for roughly a third of the network's $150 billion value. However, it is unrealistic to assume miners do not offload any bitcoin while operating, as miners sell much of their reserves to fund costs and hedge against price volatility.

If miners have sold just enough bitcoin to fund the operating and capital costs consistent with Bitcoin's historical hash rate, we estimate they have accumulated 500,000 BTC in reserves, as shown below, leaving them with less than 10% of the bitcoin they have mined over the last 5 years.[48]

Figure 14: Accumulated Reserves After Variable Costs (BTC)



Source: ARK Investment Management LLC, 2020

48 *It is important to note that the model has strong dependencies on cost assumptions, which can significantly vary.*

Adressing Mining Attack Vectors

Nation State Attacks

A major source of government power has been its monopoly on the issuance of money. As a non-sovereign money, bitcoin's existence threatens this power to such an extent potentially that nation states may respond in hostile ways.

Bitcoin's mining supply chain is an obvious target. Unlike running a node or transacting in bitcoin, industrial bitcoin mining is capital intensive and transparent. Governments, therefore, can shutter foundries, mining pools, and data centers. The Chinese government already has threatened to ban bitcoin mining.[49]

Nation states also could attempt to "51% attack"[50] the network, enabling them to censor new transactions or reverse completed ones through a "double-spend".[51] Over a long enough period of time, a sustained 51% attack could cause enough confusion to damage the network, impacting bitcoin's price and network value. The capital costs to do so would be relatively insignificant for nation states, as the sunk costs associated with mining since 2013 have totaled only $14 billion.

That said, the challenge for a nation state attacking the network would be more operational than financial. Garnering the resources necessary would be extremely difficult given the supply constraints on hardware alone and illiquid secondary markets.

Practically, the primary impediment to such an attack is the massive coordination that would be necessary between and among miners, all of whom must be willing to burn significant capital with limited guarantees of return. Moreover, if successful, the attack would render their costly hardware useless, making the high cost of acquisition difficult, if not impossible to be recouped. Consequently, the Bitcoin network never has succumbed to a 51% attack and we believe will be increasingly unlikely to do so in the future as its proof of work cumulates. Even if mining does end up more concentrated than it is today, we believe it is unlikely to break Bitcoin.[52]

Smaller chains like Ethereum Classic[53] or Verge Coin[54] have succumbed to 51% attacks in large part because their coins can be mined with generalized hardware. Yet, even after successful attacks in those cases, their network values, while impaired, did not implode.

49 *Goh, Brenda. "China Wants to Ban Bitcoin Mining." Reuters, Thomson Reuters, 9 Apr. 2019, www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4.*

50 *"51% Attack Explained: The Attack on A Blockchain." Forex Trading, Financial News, Stock Market & Quotes, www.fxempire.com/education/article/51-attack-explained-the-attack-on-a-blockchain-513887.*

51 *"Irreversible Transactions." Irreversible Transactions - Bitcoin Wiki, en.bitcoin.it/wiki/Irreversible_Transactions.*

52 *Hasu. "No, Concentration Among Miners Isn't Going to Break Bitcoin." CoinDesk, CoinDesk, 20 Feb. 2020, www.coindesk.com/no-concentration-among-miners-isnt-going-to-break-bitcoin.*

53 *Nesbitt, Mark. "Ethereum Classic (ETC) Is Currently Being 51% Attacked." Medium, The Coinbase Blog, 11 Mar. 2019, blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de.*

54 *Hertig, Alyssa. "Verge's Blockchain Attacks Are Worth a Sober Second Look." CoinDesk, CoinDesk, 6 June 2018, www.coindesk.com/verges-blockchain-attacks-are-worth-a-sober-second-look.*

Selfish Mining

Another theoretical attack on Bitcoin is selfish mining. As Vitalik Buterin describes, instead of publishing blocks to the network immediately, "*miners* [could] *selectively publish blocks, publishing many blocks all at once and thus forcing the rest of the network to discard blocks and lose revenue.*"[55] Once an attacker gains momentum with a few blocks ahead of the pack, neutral nodes join to increase their own revenue. Once this group scales to a majority, Bitcoin's network no longer is secure or decentralized.[56]

In practice, we believe selfish mining has not been and is unlikely to be an attack vector. Bitcoin miners understand that such behavior might maximize profits in the short term but will decrease their revenue and security in the long term. Additionally, miners aiming to engage in such attacks have to announce their plans and persuade other miners to participate. In response, miners could redirect their hashrate to other pools.

Quantum Computing

Quantum computers could become a threat to Bitcoin's security model and impact public-key cryptography as well as symmetric cryptography like hash functions.[57] They excel at the computations necessary to reverse one-way hash functions and to break public-key cryptography. As a result, they could render private keys insecure and help miners find new Bitcoin blocks much faster.

If it were to compromise public key cryptography, quantum computing would endanger all existing use cases: cryptocurrencies, SSL certificates, messaging apps, data storage, and more. That said, quantum computing has been ten years away from commercialization for the last 15 years, so we question how effectively during the next 10 years it will be able break public-key cryptography at all.[58]

We believe if quantum computers do become a legitimate threat, an emergency soft fork could enable the Bitcoin protocol to run on quantum-resistant algorithms. Post-quantum cryptography is an active field[59] of research,[60] with many proposals and research efforts underway.

55 *Buterin, Vitalik. "Selfish Mining: A 25% Attack Against the Bitcoin Network." Bitcoin Magazine, 7 Nov. 2019, bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440.*
56 *Eyal, and Emin Gun. "Majority Is Not Enough: Bitcoin Mining Is Vulnerable." ArXiv.org, 15 Nov. 2013, arxiv.org/abs/1311.0243.*
57 *"Schneier on Security." Blog, www.schneier.com/blog/archives/2018/09/quantum_computi_2.html.*
58 *Kim, Mark H., and Quanta Magazine. "Why Quantum Computers Might Not Break Cryptography." Quanta Magazine, www.quantamagazine.org/why-quantum-computers-might-not-break-cryptography-20170515/.*
59 *Stewart, I., et al. Committing to Quantum Resistance: A Slow Defence for Bitcoin against a Fast Quantum Computing Attack. Centre for Cryptocurrency Research and Engineering Imperial College London, London, United Kingdom, eprint.iacr.org/2018/213.pdf.*
60 *Aggarwal, Divesh & Brennen, Gavin & Lee, Troy & Santha, Miklos & Tomamichel, Marco. (2017). Quantum Attacks on Bitcoin, and How to Protect Against Them. Ledger. 3. 10.5195/LEDGER.2018.127.*

Mining "Death Spiral"

In December 2018, Bitcoin's mining difficulty dropped 15%,[61] a rate surpassed only by the 18% drop in November 2011. The magnitude of the drop created fear that Bitcoin mining had entered a death spiral. A 'mining death spiral' is a hypothetical scenario in which miners cease to find blocks. As laid out by Arjun Balaji, the argument for a miner-induced death spiral is as follows: bitcoin prices drop materially, closing down marginally profitable miners. Block times increase, slowing transactions and crushing the confidence of speculators who sell their coins, causing a further implosion in hashrate. Bitcoin blocks slow to a crawl and, because they are based on each 2016 blocks mined, difficulty adjustments render mining impossible, causing Bitcoin's "death."

Ironically, we believe mining profitability provides the case against such a death spiral. After a proof of work difficulty adjustment, miners still in the network should garner a larger percentage of the hashrate, increasing their probability of finding and profiting from the next block. As a result, higher rewards per block should compensate for bitcoin's price drop, obviating the mining death spiral.

Bitcoin's proof of work difficulty adjustment also should prevent the death spiral. Proof of work difficulty[62] measures the difficulty to hash a block. Difficulty is predetermined so that on average the hash of a block takes roughly 10 minutes. Every 2016 blocks, the Bitcoin network reassesses its global hashrate to determine whether the difficulty is consistent with the network's ability to find blocks every 10 minutes. Even during a significant drop in the hashrate prior to a difficulty adjustment, based on their contractual obligations - particularly those associated with leasing, electricity, and equipment - some miners are likely to mine at a loss in anticipation of the next downward adjustment in difficulty, preventing a death spiral.

VI. The Future of Bitcoin Mining

In our view, Bitcoin mining will become increasingly competitive. While new entrants are competing against mining and manufacturing incumbents, existing players are struggling with the commoditization of hardware and a collapse in profit margins.[63] Access to cheap energy will become further distributed as more global energy is devoted to mining Bitcoin. It will become harder to obtain larger amounts in any specific region, and regions that have historically experienced energy arbitrage opportunities will continue to be met with fierce competition. At most stages of the hardware supply chain, hardware commoditization and competition are

61 *"The 'Bitcoin Mining Death Spiral' Debate Explained." The Block, www.theblockcrypto.com/daily/4449/the-bitcoin-mining-death-spiral-debate-explained?_hsenc=p2ANqtz-84N5CTwJwY3IPCH-i8OF6p6xjgBjKhtCyEfV8ZKYZo4Ox0blUy23v1kgxphFeHhhBWQf-TApBc94Vn4HZoLwPFpERHAg&_hsmi=73263624&utm_source=hs_email&utm_medium=email&utm_content=73263624.*

62 *"Difficulty." Difficulty - Bitcoin Wiki, en.bitcoin.it/wiki/Difficulty?*

63 *"Japan's Internet Giant GMO Quits Mining Hardware Bussiness." Bitcoinist.com, 26 Dec. 2018, bitcoinist.com/japans-internet-giant-gmo-quits-its-mining-hardware-bussiness/.*

lowering the risk of monopolies, a promising sign for Bitcoin. There, however, remains a high level of concentration at the foundry level. Only two - TSMC and Samsung - have the resources and skills to deliver cutting edge fabs. Over time, fabless designs should become more efficient, lowering the foundries' bargaining power. As ASIC lifecycles continue to lengthen, the need for miners to rely on manufacturers may also diminish. At the mining pool level, while there may be increased concentration risk, efforts to further decentralize hashpower at the protocol level are underway. And, as as we've noted, mining concentration does not necessarily yield a greater risk to security.[64]

While considered a risky, volatile but highly profitable business today, we believe mining should evolve to resemble the traditional commodities industry over the long term. ASIC lifecycles will be long enough that industrial miners will have far greater predictability on their cash flows. In a mature derivatives market, miners will be also be able to hedge against bitcoin's volatility risk, ensuring sufficient cash flows to fund ongoing operations. The greater predictability will attract a new pool of risk averse players with large sums of capital. These players will further capitalize on the second and third order opportunities mining presents. One such example is its usefulness in smoothening peak and trough power demands. While many power plants tend to only run during times of peak energy demand, Bitcoin mining provides incentives to operate year round.[65] Ultimately, deeper capital markets, longer hardware cycles, lower than expected thresholds to profitability, and dampened price volatility should provide significant opportunities to unlock an unprecedented demand to mine bitcoin.

In its entirety, we estimate the cumulative spending on mining (17 billion USD) is just above 10% of the total wealth it secures (150 billion USD), of which the energy burned to secure Bitcoin annually is a fraction. Viewed under this lens, the mining industry has become hyper-efficient in the relative amount of resources it expends as a function of the wealth it has secured to date. We expect Bitcoin's network value to continue to appreciate at a faster rate than cumulative mining spending, yielding even greater efficiencies than today.

In times of geopolitical uncertainty and financial market volatility, converting electricity into a monetary asset could take on new importance. We believe Bitcoin is a call option on a global digital monetary system and a hedge against existing regimes, potentially undermining the dollar as the world's reserve currency. Bitcoin mining could be the ultimate path to direct exposure to this new monetary world order.

64 *Hasu. "No, Concentration Among Miners Isn't Going to Break Bitcoin." CoinDesk, CoinDesk, 20 Feb. 2020, www.coindesk.com/no-concentration-among-miners-isnt-going-to-break-bitcoin.*
65 *"This Utility Heats New York State—And Mines Its Own Bitcoin" Bloomberg, 5 Mar. 2020, https://www.bloomberg.com/news/articles/2020-03-05/this-utility-heats-new-york-state-and-mines-its-own-bitcoin*

ARK Invest Management LLC
3 East 28th Street, 7th Floor
New York, NY 10016

info@ark-invest.com
www.ark-invest.com

Join the conversation on Twitter @ARKinvest