



Analysis on Monero Mining

07.01.2018

Timothy Miller


The Ved.io Group, LLC
626 Grist Mill Rd.
Stanford, KY 40484

Overview

Federal Reserve

In November 1910, wealthy bankers, including representatives of J.P. Morgan, met on Jekyll Island to draft the Aldrich Plan, which would lead to the creation of a U.S. Central Bank. The Aldrich Plan failed to pass the Senate, but this did not deter the bankers. As special interests groups often do today, the bankers rebranded and revised their bill. While the Aldrich Plan had no limits on banking interest representation, regulation was introduced in the Glass-Owen Bill with the creation of the Federal Reserve Board (FSB). The Glass-Owen Bill mandated a small percentage of the FSB be elected by Washington D.C. Today, the FSB consists entirely of representatives for banker interests. There was also one important, often overlooked modification. Instead of the proposed currency being an obligation of the private banks, the new Federal Reserve note was to be an obligation of the U.S. Treasury. The Glass-Owen Bill passed as The Federal Reserve Act on the eve of Christmas Eve, 1913.

The Federal Reserve Act mandated all nationally chartered banks accept stock in the Federal Reserve. In 1971, President Nixon took the U.S. (bankrupt from the Vietnam War) off the gold-standard. Now, the U.S. Treasury, overseen by the banking industry, can introduce as many bonds as they please. Bond comes from the root word bondage. The U.S. Central Bank system is enslaving the population with unpayable debts. The legislation gave three families who owned 25% of the world's gold supply, at the time, control of the U.S. monetary supply to prevent events like the Panic of 1907. Today, the Federal Reserve is still a private corporation with owners. Throughout the years there has been a confusing series of mergers and acquisitions so who exactly owns the Federal Reserve is a closely guarded secret. We know, however, that Federal Reserve stock was initially issued to the largest banks in the United States, which means Chase (JP Morgan), Citigroup (Rockefeller), and Bank of America (Rothschild). Hidden on the Federal Reserve website (<https://www.federalreserve.gov/aboutthefed/section7.htm>), Federal



Reserve stockholders are entitled to an annual 6% dividend for indebting the public. Mike Maloney, founder of goldsilver.com, describes the system, “The banks get to make a profit by selling part of our national debt, bonds, to the federal reserve who buys them with a check from nothing. Then we pay tax to pay the principal, plus interest.” Most of the world uses US Dollars as a reserve currency. The flow of US Dollars is controlled by the Federal Reserve. The Federal Reserve of the United States is under control by the banks. So the Chase, Rothschild, and Rockefeller families essentially control the global financial system.

“Permit me to issue and control the money of a nation, and I care not who makes its laws!”


- Mayer Amschel Rothschild

There is a fascinating series about the history of money by Mike Maloney here: <https://www.youtube.com/watch?v=iFDe5kUUyT0>

Blockchain

Blockchain enables for the first time in history a protocol to exchange value with anyone on the internet without trusting a centralized institution. When asked to describe the significance of blockchain technology, Vitalik Buterin (Co-founder of Ethereum) said, “Money is something a community can make for itself whenever it wants”. People are starting to tokenize assets on blockchains to facilitate a trustless peer to peer exchange of fungible and non-fungible assets, such as gold and art. To achieve a trustless protocol, consensus over the current state of the blockchain (order of the transactions) needs to be reached. There are a number of consensus algorithms in use on a variety of blockchains around the world, the most mature and popular being Proof of Work. Today, we are interested in understanding the profit potential of turning electricity into computational power on a PoW blockchain.

Mining




Energy is never burned or wasted using PoW. No miner is wasting energy, they get paid for their contribution, and that contribution is proportional to the usefulness and value of the network as a whole. Miners are rewarded with cryptocurrency as incentive for providing hashrate to the network. In the context of cryptos, hashrate is the speed at which a computer is completing an operation on the crypto network. Miners are just bank tellers who process our checks for us and update the banking ledger. But instead of being paid by the bank that owns the ledger, miners are allowed to create small amounts of coins for themselves as a reward for their bank teller work.

The process of mining on PoW is as follows:

1. Miner validates the cryptographic signature of all transactions it wants to include in the block to be added to the blockchain.
2. From the valid transactions, the miner calculates their [Merkle root](#), which becomes the block's header field.
3. The miner repeatedly hashes this header, modifying its nonce field with each try. In cryptography, a nonce is an arbitrary number that can be used just once.
4. When the miner finds the correct hash, the miner appends this block (including the block's header and transactions) to the blockchain. This is also referred to as "solving a block"
5. The miner who found the correct hash is rewarded with crypto.

Miners create blocks at the block time rate of the particular PoW crypto. The block time is an average time. It is a measure of how long it takes the hashing power of the network to find a solution to the block hash. The difficulty of the block hash problem is adjusted automatically on a fixed interval to scale with the total network hashrate such that the problem is solved, on average, in a block time interval.

The mining node which discovers the correct hash is allowed to create new crypto in what is called a coinbase transaction. A coinbase transaction is a type of transaction where new crypto is created for the purpose of creating economic incentive to run a mining node and be a good actor. The theory behind why miners have been good actors so far is because the



infrastructure cost required to mine a new block consistently means it is in the miner's best interest to provide a safe experience. A malicious miner with 51% of the mining capacity can double spend crypto or issue a denial of service attack to prevent new transactions from being added to the blockchain.

Because there is a small chance a malicious actor with little investment into mining hardware can mine the next block, it is standard to wait for multiple blocks to be added to the blockchain before a transaction is considered finalized and correct. Someone with 51% or more of the mining capacity is the only person who would have a significant percentage chance at mining 3 or more blocks in a row, in order to add their maliciously modified blocks to the blockchain and be accepted by the community.

There are a lot of mining nodes competing for the block reward, and it is a winner take all scenario. Because of this, miners often create what are called "pools", or a group of miners who share in the profits from mining a block. For example, if Alice were solo mining with 20% of the network capacity, she should expect to append one out of every five blocks. This means she experiences four block times of unpaid work. To gain consistent block rewards, Alice may join an existing mining pool with 50% of the mining capacity and get paid for her share of the total mining pool hashrate, more consistently, every other block time. Mining pools have owners, and they usually charge a percentage fee (1-3%) from those mining in their pool

Existing Work

Mining



[Remains of an crypto mining farm in China following a flood - c. 2018](#)

Crypto mining can be simplified to a combination of three distinct games:

1. ASIC design
2. Cost of manufacturing
3. Cost of electricity

Miners seek to maximize profit by maximizing the performance of their computer hardware, measured in hash per watt, and seeking access to low cost electricity. Demand for higher hash per watt drove miners to design specialized hardware called ASICs. If you rated the performance of mining equipment on a scale of 1 to 10, 1 would be an Intel CPU, 10 would be an optimized ASIC, and 2 would be a GPU.

Using a vending machine as an example, a highly optimized ASIC would have only the logic required to process nickels, dimes, and quarters embedded in its circuits. When powered on, it serves one task (whatever it is programmed to do in hardware), but it does it quickly and efficiently.

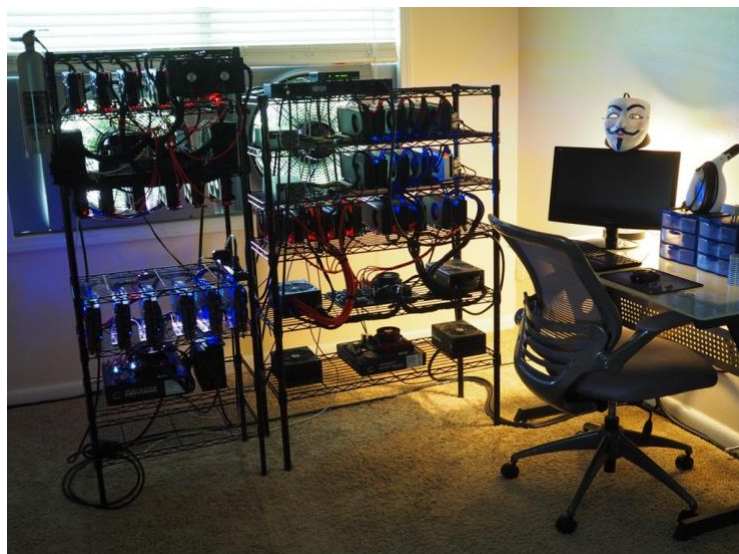
$$\text{Efficiency} = \text{performance} / \text{resources}$$

Performance is measured in hashrate and resources are watts of electricity.

Contrast this to a general purpose CPU, which uses cores. In computer science, a core is any computing unit able to fetch, execute, and store instructions. These cores read instructions written in code to manipulate their registers. This simulates the logic described in the instructions, in software. Each of these steps has levels of abstraction that enable it to handle many types of operations, but at the expense of speed and efficiency.


A GPU is designed to handle operations necessary for processing graphics or machine learning such as [multiply-accumulate](#). A GPU might have a general purpose CPU for handling a wide array of instructions, but an integrated ASIC for multiply-accumulate operations. This provides flexibility of instructions, but speed and efficiency for a few select operations.

Bitmain, a Chinese company, is the market leader in ASICs. Because ASICs are essentially money printing machines to a miner, Bitmain will not sell their ASICs to anyone for less than they can profit from using it themselves. This leads to many PoW crypto projects being ran almost exclusively on ASICs, and centralized to companies like Bitmain. To be cost effective, an ASIC needs to be made in a Chinese factory. Other companies have tried manufacturing their ASIC designs in China, but have been denied as Bitmain has connections to all the manufacturing capacity in China.



[Residential Crypto Mining Operation - c. 2018](#)

A PoW network would be considered more decentralized and thus healthier if it had 100 miners at 1% capacity each, rather than 1 mining 60%



of the capacity and the other 99 sharing the remaining 40%. This is because it helps prevent from a 51% attack, described earlier in this paper. Many cryptocurrency projects realize the importance of keeping ASICs off their PoW network. One such project is the privacy coin Monero.

Why Monero

[The Monero Project](#) created the [Moneropedia](#) to educate those interested in how Monero works. When I make references to Monero developers, I am referring to the developers representing The Monero Project. The Monero Project is a loose collective of individuals behind Monero.

Monero is the best crypto to mine because it solves real world problems, is ASIC-resistant, and will stay PoW for the foreseeable future. There are over 1,500 crypto projects in the wild. These projects are categorized by the problems they solve. Monero is a member of the privacy coin space, or cryptocurrencies that provide users with a higher level of anonymity. Monero's closest competitor in the privacy coin space is Zcash. The Zcash whitepaper describes the purpose of privacy coins:

“Privacy guarantees are designed to benefit legitimate users who do not want their financial details made public. There is a concern, as always, that decentralized anonymous payments will facilitate the laundering of ill-gotten funds by criminal users....however [Privacy coins] barely affects the status quo for criminal users, who already have strong incentives to hide their activity, while it provides notable benefits to legitimate users.”

Arguments for Monero over Zcash I've heard are

1. Since privacy is optional, private transactions stick out from the rest. All Monero transactions are private.
2. Zcash requires a trusted setup ([which may be compromised](#)), Monero does not
3. Zcash is a venture capital funded company, Monero was created by a loose collective of individuals.


- 
4. Zcash takes a percentage of all miner's profit as "revenue" for itself. Monero does not.

Zcash's CEO has made alarming comments, such as [publicly declaring he is open to helping the government track suspicious activity](#). The guy is paid \$4 million a year, more than most fortune 500 CEOs.

Monero is an open-source cryptocurrency created in April 2014 that focuses on privacy and decentralization. Monero is the cryptocurrency most like digital cash since it is peer to peer and anonymous. In the Monero network, all transactions are private by default and no one knows the quantity in anyone's wallet unless the owner discloses that information. Monero is fungible, meaning that every unit of the currency can be substituted by another unit. This makes Monero different from public-ledger cryptocurrencies like Bitcoin, where addresses with coins previously associated with undesired activity can be blacklisted and have their coins refused by other users. This happened to the hackers behind the "WannaCry" ransomware who tried to convert their ill-gotten Bitcoin into Monero on the crypto exchange ShapeShift, and were denied. Some Bitcoin addresses, such as the "WannaCry" ransomware addresses, are well-known. If you receive coins tainted by these "bad actors", you may have trouble selling them later. In practice, this effect has been limited. It is not really reasonable to expect all merchants to blacklist tainted coins.

Monero solves this problem by implementing [Stealth Addresses](#), which allow and require the sender to create a random, one-time address for every transaction on behalf of the recipient. From the blockchain data, no one can tell who sent Monero to who, but the sender and recipient can verify for themselves the balances of their [wallet](#).

Monero's developer community is active. An active developer community is good, because it shows a unified effort to improve the project. When there is a change made to the network, a hard fork on the code base happens, where the project splits into two versions, the old and the new. The majority of the developers continue to work on the new version, which prevents a fragmented ecosystem. As far as privacy coins are concerned, all the potential people innovating to replace Monero as a privacy coin are



working on improving the Monero project itself. For example, Monero transactions prioritize privacy over keeping transactions small (On-chain transactions for Monero are almost 40 times as large as Bitcoin). On-chain transactions are transactions which are added directly to the blockchain, instead of passing through a relayer. Off-chain transactions lower transaction costs by aggregating transactions into one transaction, at the expense of decentralization. The size of the block, which contains transactions the miner adds to the blockchain, is a fixed size. As such it can only handle a certain number of transactions. As a result, Monero would encounter scaling problems from increased transaction volume under smaller volumes of transactions than Bitcoin. As new features are created by the community, such as mimblewimble (a solution to lowering transaction sizes to solve the scaling problem of on-chain transactions), they are added into Monero's codebase, instead being available exclusively on a competing, new crypto project.

When Monero needs money to fund development, it asks the community for donations. This allows users of Monero to determine the direction development of the cryptocurrency takes. It is important that all transactions be private in a privacy coin blockchain because if an investigator wants to deanonymize transaction history, the private transactions stand out as irregular, while information can be gained from the non-private transactions. Privacy coins are a controversial topic these days because of the potential for money laundering and “know your customer” policies at financial institutions. It is possible, however, to exchange Monero for any other crypto on an exchange. It may be in a Central Bank's best interest to shut down a project like Monero, but they cannot because the theoretical cat is already out of the bag. Monero is open source, so anyone interested can build upon it, it serves a purpose, the mining model is decentralized, and exchange is done peer to peer. [See the number of transactions on the Monero network here.](#)

Monero has adopted ASIC-resistance as one of its top priorities. This is to encourage the use of more easily accessible GPUs for mining. As a miner, the benefits of using GPUs over ASICs are:

1. Warranty period


- 
2. Accessibility
 3. Resale value

Monero Mining Algorithm

Monero uses CryptoNight as its Proof of Work mining algorithm. CryptoNight comes with a few features that are worth keeping in mind. Most notably, CryptoNight is particularly memory intensive. CryptoNight was designed with modern CPUs in mind. For example, the CryptoNight algorithm performs operations that make a high utilization of the 2MB L3 cache on Intel CPUs. Because of this, GPUs and ASICs are not always faster than CPUs at mining. As a result, [Crytonight benefits the casual miner by reducing the payoff received from specialized hardware](#). The reason GPUs are used in CryptoNight mining is because finding a motherboard with support for more than two CPU sockets is rare, while connecting 8 GPUs on a single motherboard for crypto mining is common to find in mining operations. Because of this, GPU mining allows for a higher hashrate per dollar.

Bitmain ASICs

Bitmain designed an ASIC to secretly mine Monero for themselves, without making the machines commercially available. The ASICs become paperweights when the developers instated a six month hard fork schedule for updating the algorithm to maintain ASIC-resistance. Developers behind the crypto project SiaCoin have claimed ASIC-resistance is futile because ASIC designs can be generalized at the expense of performance, but to the benefit of saving months in engineering time for the ASIC design phase. Others have proposed optimizing the hashing algorithm to perform best on generalized hardware, so ASICs would yield only a marginal improvement. The CryptoNight algorithm, which powers Monero, actually performs best on high core count CPUs, with the cache size of current gen CPUs such as [AMD Threadripper](#) (a 16 core CPU). CryptoNight was designed to be mined on




modern CPUs. The reason why GPUs are more efficient for mining is because certain motherboards can handle up to 20 GPUs, which saves cost on the amount of RAM sticks ([RAM prices have doubled in the past year](#)), power supplies, storage, and motherboards required. By contrast, it is rare to find a motherboard that holds two CPUs, referred to as a dual-socket motherboard.

The cost of custom made ASICs can reach tens of millions of dollars and months of engineering work. [SiaCoin wrote an excellent blog post about their experience designing an ASIC and their subsequent exit from the industry because of Bitmain's business practices.](#) Basically, Bitmain's employees are smart and they play dirty.

Regardless, it is clear that months of expensive engineering work go into designing an ASIC, and Monero will do anything it can to fend off ASICs. We can see from the Monero network hashrate chart that since changing the algorithm, the difficulty of mining a block has gone way down. I imagine Monero will speed up the algorithm swap time to a time more frequent than 6 months should ASICs become a problem in the future. Bitmain is the dominant player today, but such a lucrative business has attracted competition from firms like Intel. Engineering talent for designing ASICs is in demand and very rare. My guess is Bitmain is strapped for engineering talent as is, and will move onto easier, more profitable prey such as Bitcoin as designing and optimizing for a platform that changes every n months is definitely demoralizing and expensive.

GPU Mining

GPUs are manufactured by either AMD or Nvidia. Mining the current algorithm behind Monero is the most profitable on the AMD Vega 64. When mining an ASIC-resistant coin, the first two games (ASIC design and manufacturing) are eliminated, leaving only the cost of electricity. Without diving into the speculative world of cold fusion, some of the cheapest energy sources in the world are hydroelectric, nuclear, Mexican solar, and American coal. From my research, the lowest hydroelectric miner is paying \$25 per MW/h. Additionally, anything below \$20 per MW/h is the top 1% cheapest




electricity in the world. Because of the competition for cheap electricity, many in the community have been forecasting the centralization of miners where individuals will no longer mine residentially, only in large scale centralized mining farms. Mining will become centralized when it becomes unprofitable to mine using residential energy. However, it will never become unprofitable for the miners using the cheapest electricity and most efficient hardware, as PoW works by incentivising miners to give their hashrate to the network. If it is unprofitable for the cheapest producer, there is no incentive, which would mean nothing short of total collapse of the cryptocurrency.

Preferably, the mining operation would be in a cool, dry climate so air from outside could be blown over the hot GPUs. Mexican solar may be cheap, but the hot, dry environment would mean paying for expensive air conditioning.

Both AMD and Nvidia are making boatloads of money selling their GPUs to miners, which were designed for tasks such as AI and gaming. This has led to a surge in aftermarket GPU prices, and unhappy computer scientists who cannot get their hands on affordable high performance computing. It is speculated that AMD and Nvidia are working on GPUs specialized for mining. Nvidia's hardware is supposed to become commercially available sometime in late August. With it's last release, Nvidia doubled performance for slightly more money. This year's release is expected to be equally as disruptive for the AI and gaming space. For the workload of Monero mining, I don't think Nvidia's GPU release will bring radically improved efficiency, however. AMD's roadmap is much more interesting. AMD is releasing a 7nm version of Vega GPUs this year and early 2019, down from 14nm the year before. This means more performance for less power consumption. This would be an especially good time to upgrade as the 7nm manufacturing size will not be superseded for at least three years according to [AMD's GPU roadmap](#)

Ethereum Mining Wave

Ethereum is moving from PoW to Proof of Stake (PoS) in late 2018, early 2019. Proof of Stake is a consensus algorithm in which miners don't



allocate computing power, but instead their stake in the crypto to vote on consensus. PoS does not require mining hardware, and rewards those who acquire the largest stake in the crypto with block rewards. PoS requires disclosing your wallet address to determine your stake in the ecosystem. This is incompatible with Monero, because of Monero's use of [stealth addresses](#), an important part of Monero's inherent privacy.

Today, Ethereum is frequently the most profitable PoW coin to mine. When Ethereum makes the switch to PoS, a subset of the GPUs mining Ethereum will allocate their hashrate to other PoW blockchains to try and make a profit. This may lower the overall profit for miners on Monero. Regardless of the hypothetical flood of mining capacity we understand that given the same hardware, mining becomes a game of cheap electricity. Most online articles are spreading news that "mining is dead" simply because it is becoming less profitable to mine on \$120 MW/h residential electricity.

Goal

1. Maximize profit for electricity production

Specifications

In this paper, I estimate the financials for a proposed optimal mining setup consisting of 12 to 100,008 GPUs

Cooling

Appalachia has up to 90% humidity on the worst days. Typically, it is not safe to operate computer hardware in an environment above 80% humidity. Air conditioning may be prohibitively expensive, and cut into profits. Recently, a cottage industry has erupted around exotic mining computer cooling. One such solution, which would be independent of humidity is to submerge the hot GPUs in non-electrically conductive mineral oil, which is cooled via heat exchanger from nearby river water. Little to no electricity would be necessary for cooling. The picture on the cover of this paper shows a mining rig submerged in mineral oil.

[An example of the mineral oil setup can be found here](#)

Variable Costs

Each computer, referred to as a mining rig, is the unit in which the mining operation scales. Each computer has 12 GPUs, the maximum amount supported by Windows at this time. Fitting the most GPUs per motherboard has obvious cost advantages, but tradeoffs in stability can occur. When one GPU freezes, the whole system could stop mining. The mining software can run on unactivated versions of Windows 10 in a headless configuration. Currently, AMD releases their blockchain driver for Windows only. This makes mining Monero with AMD hardware more efficient. The linux drivers for AMD Vega 64 don't get the same performance as the Windows drivers, at around 67%. This means the popular linux operating system for miners, [ethOS](#), cannot be used for running the mining software off of a USB. This also means a hard drive is needed for each machine. This may change in the future, as AMD is refining the Vega platform this year by moving the manufacturing process from 14nm to 7nm, and additional driver improvements could happen.

These prices are from Amazon. Cheaper prices can be had if negotiating hardware purchases from the manufacturer. The computer parts for each rig are as follows:

Part	Model	Price
Motherboard	Biostar Motherboard TB250-BTC PRO	\$103.97
Processor	Intel Celeron G3900	\$37.22
RAM	4GB RAM	\$41.99
Storage	60GB SSD	\$19.99
Power Supply #1	400 watt PSU for motherboard	\$33.36

Power Supply #2	2 x 1200 watt PSU for GPUs	2 x \$99.00 = \$198
Adapters	4 x 6-pin to 8-pin adapter	4 x \$3.25 = \$13
GPUs	12 x AMD Vega 64	12 x \$499 = \$5988
Total		\$6435.53 + 6% tax = \$6821.66

Power efficiency = Power provided to internal components / amount of power drawn from the wall

The efficiency rating of power supplies are listed below. The 1200 watt power supply is rated 80 Plus Platinum. The 400 watt power supply is rated for 75% efficiency.

Efficiency level certifications [\[edit \]](#)

THE SWEET SPOT


80 Plus test type ^[4]	115V internal non-redundant				230V internal redundant				230V EU internal non-redundant			
Percentage of rated load	10%	20%	50%	100%	10%	20%	50%	100%	10%	20%	50%	100%
80 Plus		80%	80%	80%						82%	85%	82%
80 Plus Bronze		82%	85%	82%		81%	85%	81%		85%	88%	85%
80 Plus Silver		85%	88%	85%		85%	89%	85%		87%	90%	87%
80 Plus Gold		87%	90%	87%		88%	92%	88%		90%	92%	89%
80 Plus Platinum		90%	92%	89%		90%	94%	91%		92%	94%	90%
80 Plus Titanium	90%	92%	94%	90%	90%	94%	96%	91%	90%	94%	96%	94%

Actual power consumption from the wall would be around

[Image Source](#)

$$50 + ((160 * 12) / 0.90) = 2183.33 \sim 2184 \text{ watts}$$

The GPUs consume $160 * 12 = 1920$ watts, but the power must be converted from AC to DC at a rate of 90% efficiency (the server PSUs are rated for 94% efficiency best case scenario, 90% worst case scenario). The 50 watts is the estimated power draw from the rest of the system, which will not consume too much power because it is not used in the mining process.



We want to run at peak efficiency, so we aim for an 80% load on each PSU. Regarding power supply efficiency ratings, an 87% efficient Gold rated 750W PSU will pull 862W at the wall while outputting 750W. The server power supplies require 240V outlets to get their full rated output capacity.

The single 400 watt power supply requires a 120V outlet. The 400 watt power supply is the cheapest way to power the rest of the computer components, because special power connectors are required (24-pin, etc) and clean, consistent power needs to be fed to the system for stability during 24/7 operation.

- Each Vega 64 requires 2 x 8 pin connectors
- Server power supplies are the cheapest for high watt requirements. Breakout boards only support 6 pin connectors. We need 24 6-pin to 8-pin adapters. The server power supplies come with 8 x 8 pin adapters, so we need to buy 4 more to connect power to all the GPUs.
- Each Vega 64 can mine at a rate of 1990 H/s @ 160 watts.

Efficiency ratings for Monero mining came from [this guide](#).

Other variable costs

There are some variable costs that are not accounted for such as:

1. Cost of cooling
 - a. Dielectric mineral oil
 - b. Heat Exchangers
 - c. Computer case

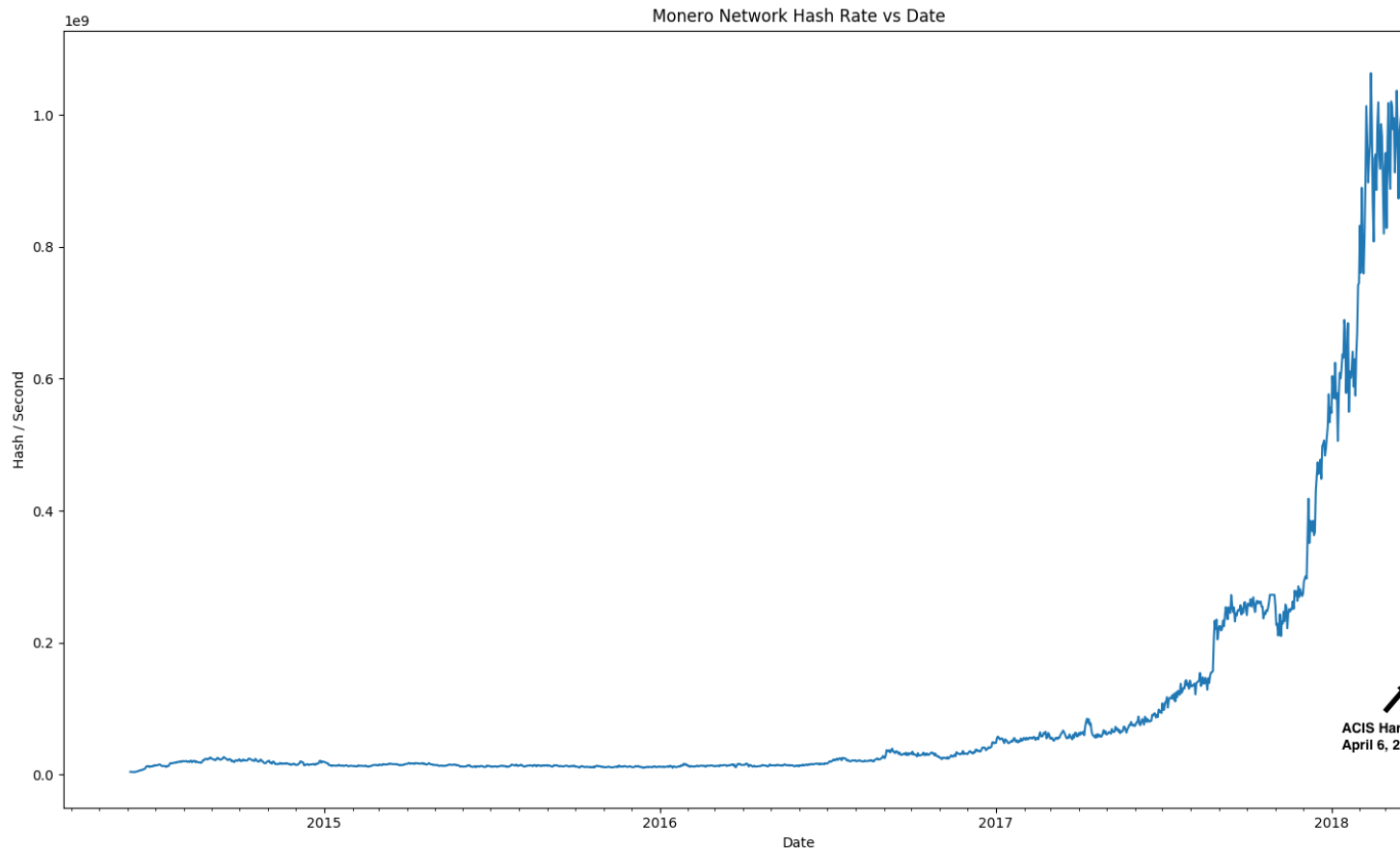
These costs can be shared across mining rigs, as the GPUs will sit in a shared tank of mineral oil that is pumped over the heat exchangers to cool.

Fixed Costs

There are certain fixed costs that are hard to estimate as they depend on the location.

1. Electrical infrastructure for 240V and 120V outlets
 - a. Each rig requires two 240V plugins and one 120V plugin
2. Security infrastructure to protect the mining rigs

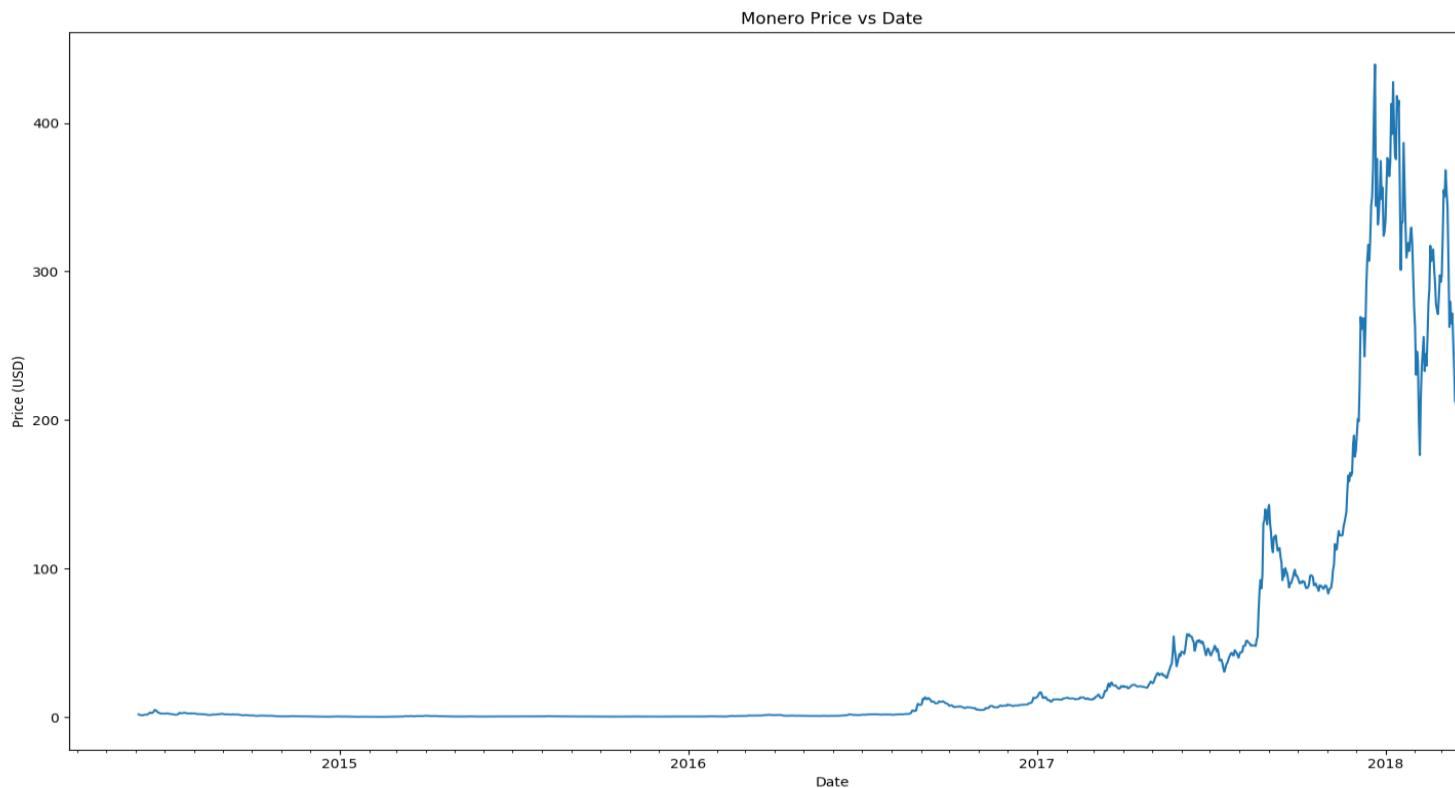
Data

[View Full Size Image](#)[View](#)[Data Source](#)

Monero Network Hashrate

This chart shows the hashrate of the Monero network since inception. The hashrate rose in late 2017 because the increase in price made mining more profitable, so more miners got involved. The hashrate dropped off significantly in April 6, 2018 because Monero developers were concerned Bitmain may have created an ASIC capable of mining Monero, and was mining in secret. ASIC mining is seen as a security vulnerability ([see 51%](#)

[attack](#)) by Monero developers, so they agreed to change the mining algorithm every six months to make it difficult to design an ASIC for the current mining algorithm and then mine for a long enough time to recoup investment on the ASIC design.



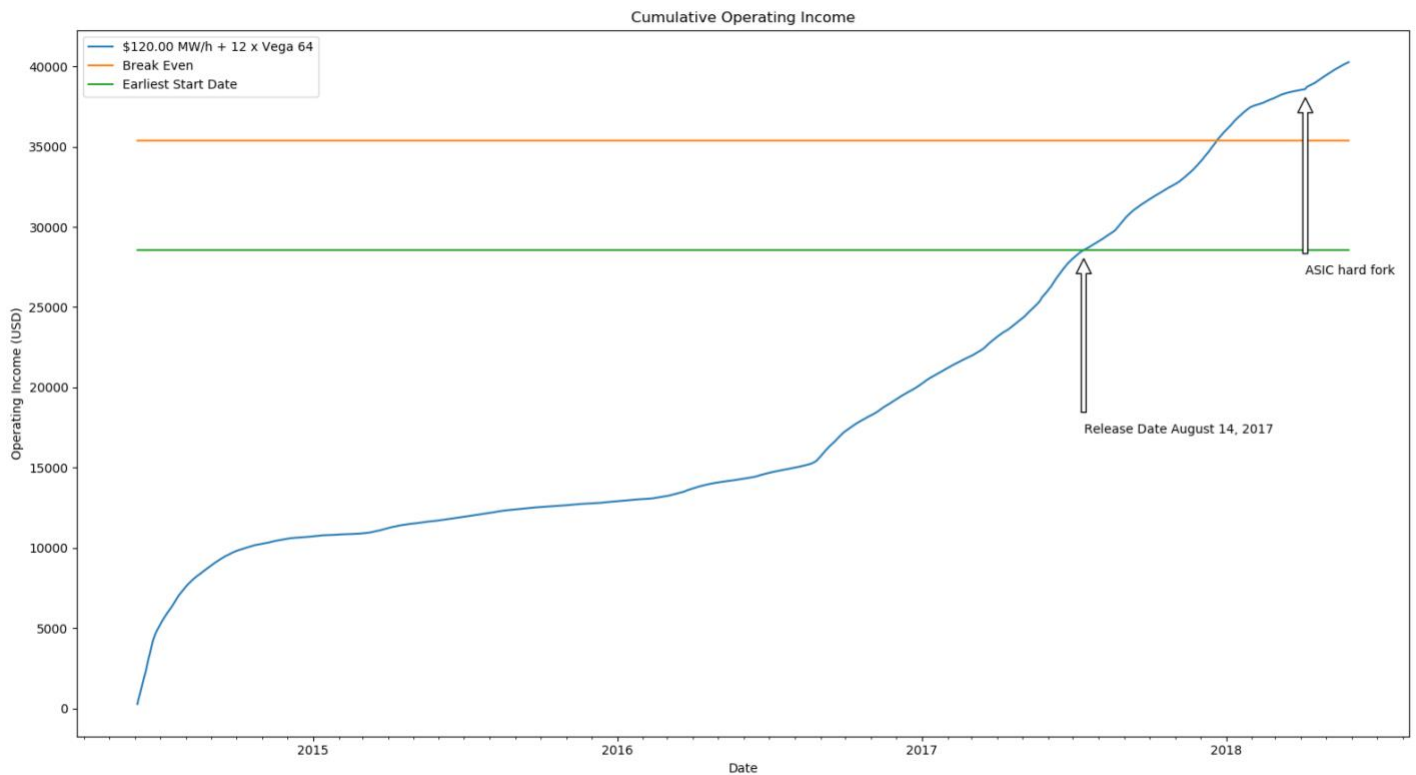
[View Full Size Image](#)
[Data Source](#)

[View](#)

Historical Monero Price

This chart shows the price of Monero since inception. You can see the price of Monero is highly volatile. You can also see after the hard fork a positive correlation between price and network hashrate. This could be because

small miners are exiting the market to sell their GPUs to maximize profit. The falling Monero price spooks them, and the next GPU update cycle is approaching. Nvidia is speculated to have new GPUs launching between late July and August. Regardless, this trend means the operating income in US Dollars from mining remains strong, despite the rapid fall in price of the underlying asset.



[View Full Size Image](#)
[Data Source](#)

[View](#)

Cumulative Operating Income (Residential)

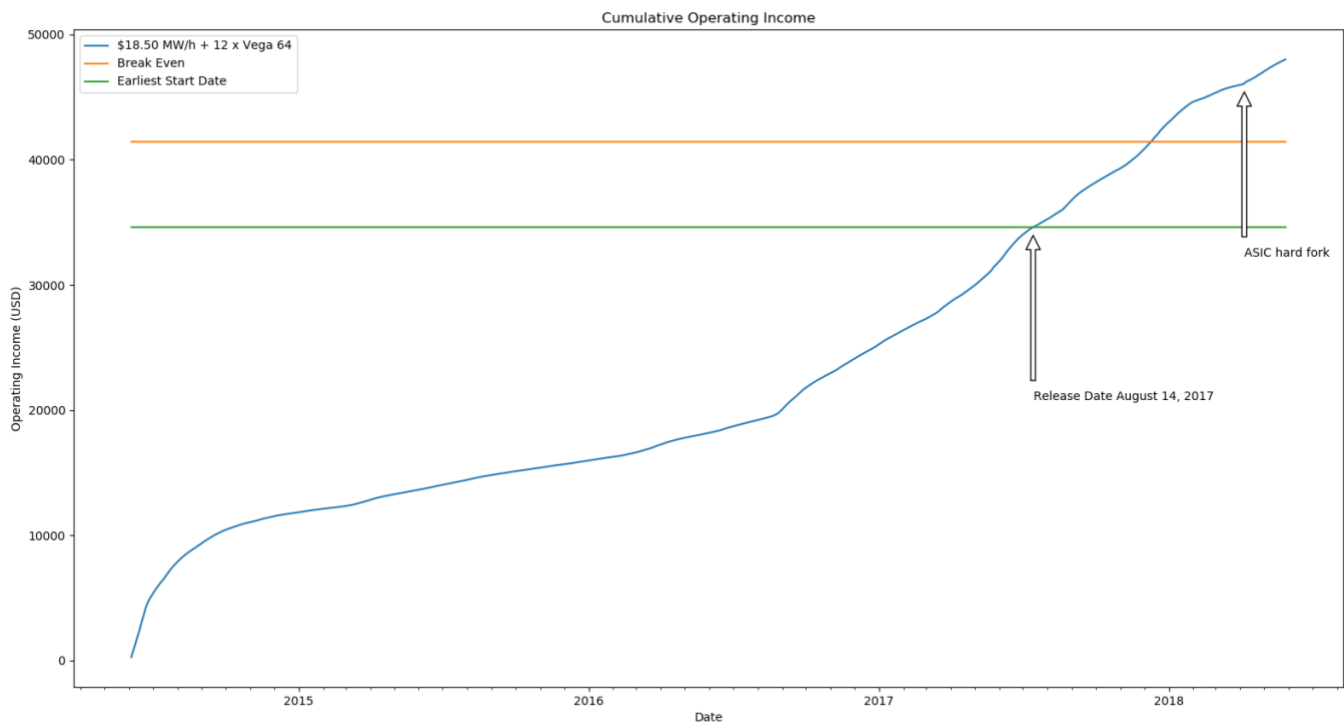
This chart shows cumulative operating income for a mining rig consisting of 12 AMD Vega 64, using residential energy at the rate of \$120 MW/h.

Green Line

Launch date for the AMD Vega 64 GPU, the component performing the mining calculations. The data before this date is nonsensical, because the hardware was not available before then.

Orange line

Break even point where the cumulative operating income equals variable costs (consisting of one mining rig as defined in the Variable Cost section). The GPUs operate independently, but share the other computer components such as CPU and RAM. This means mining rigs would be most cost effective in increments of 12 GPUs.



[View Full Size Image](#)
[Data Source](#)

[View](#)

Cumulative Operating Income (Coal)

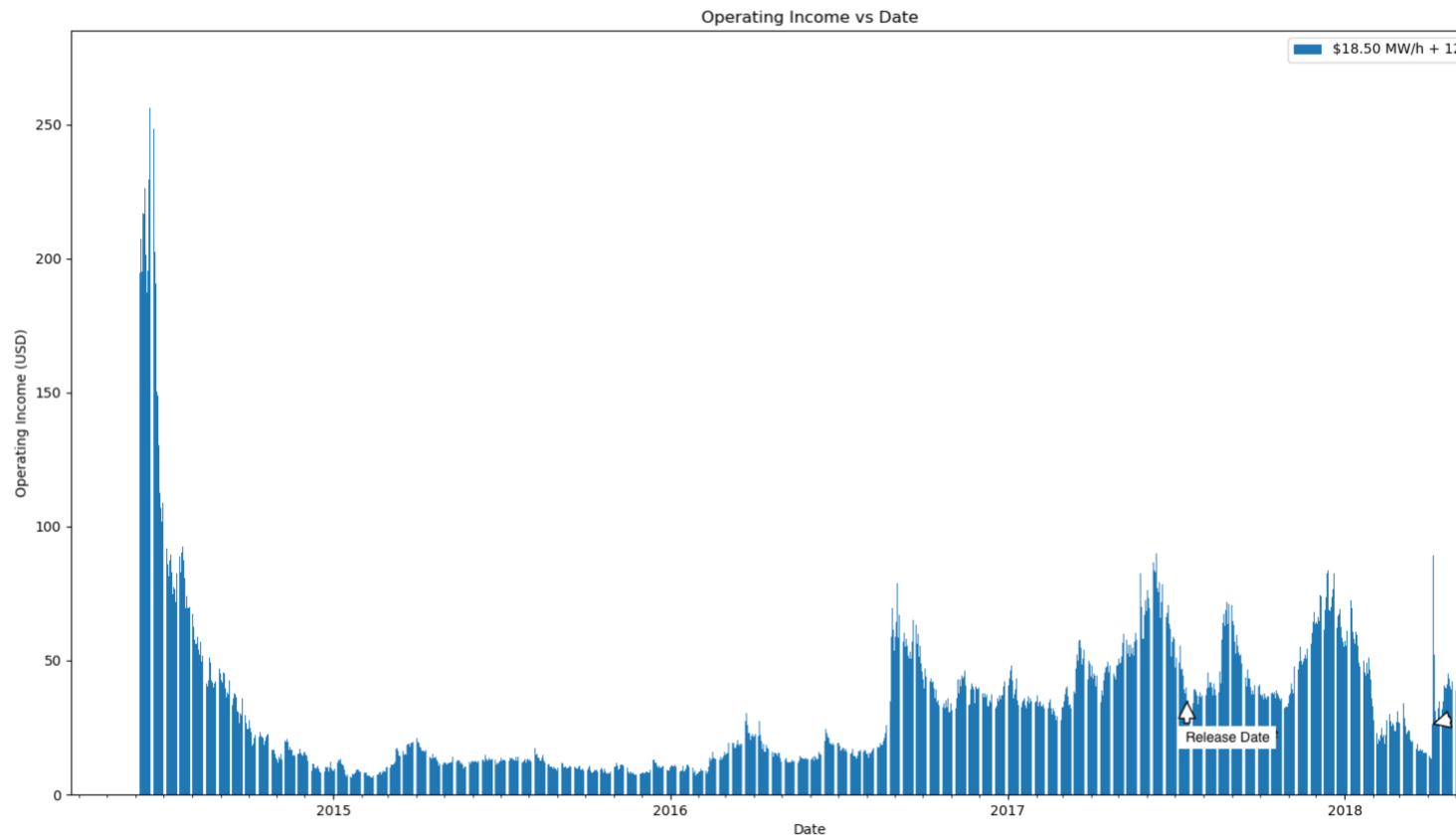
This chart shows cumulative operating income for a mining rig consisting of 12 AMD Vega 64s, using coal at a rate of \$18.50 MW/h.

Green Line

Launch date for the AMD Vega 64 GPU, the component performing the mining calculations. The data before this date is nonsensical, because the hardware was not available before then.

Orange line

Break even point where the cumulative operating income equals variable costs. When the Monero developers agreed to change the mining algorithm every six months on the “ASIC hard fork” point, profitability increased for all miners not using ASICs. This is because ASICs are very efficient, and gain an unfair advantage over non ASIC miners in terms of hash per watt. When the ASICs were suddenly removed from the network, the percentage of the total network hashrate for each miner increased, so their share of the block reward increased. The variable costs are the same for the coal and residential cumulative operating income graphs. The scale is different in the Y axis because the coal graph has a larger cumulative operating income.

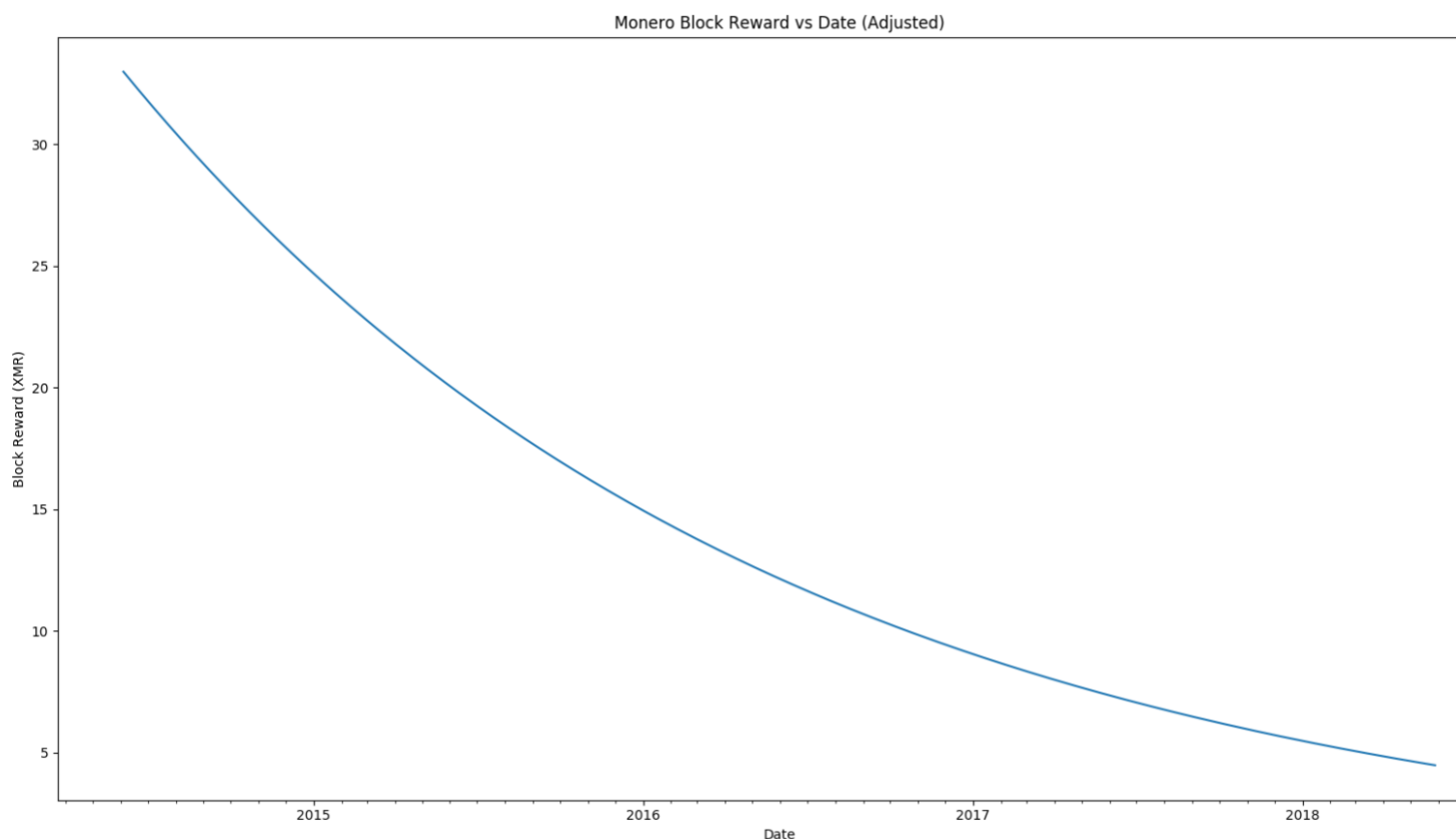


[View Full Size Image](#)
[Data Source](#)

[View](#)

Daily Operating Income (Coal)

This chart shows daily operating income for a mining rig consisting of 12 AMD Vega 64s, using coal electricity at a rate of \$18.50 MW/h. The applicable data is from the X position labeled Release Date, onward. Operating income improved after the mining algorithm change forced ASICs off the network. As discussed earlier in the paper, operating income must remain positive for the lowest cost electricity producer, assuming equal efficiency mining hardware. Without incentive, the miners have no reason to provide security to the network.



[View Full Size Image](#)
[Data Source](#)

[View](#)

Monero Block Reward

This chart shows the adjusted Monero block reward since inception. The chart is adjusted because on March 20th, 2016 the time for creating a new block was doubled from [one minute to two minutes](#). A Block Reward is the amount of crypto a miner receives for solving a block. [Tail Emission](#) is the name for Monero's block reward system. According to Moneropedia:

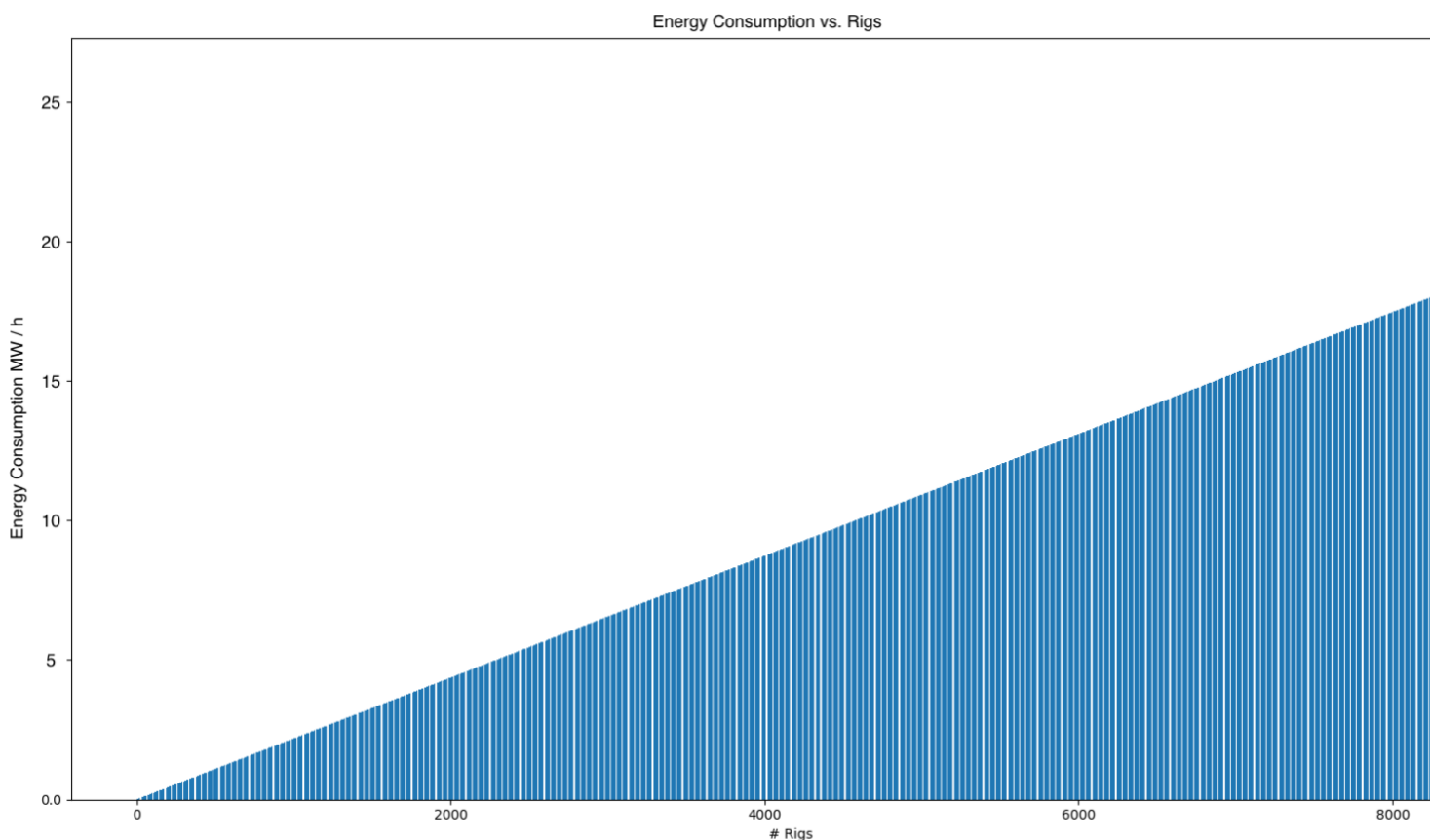
“Monero block rewards will never drop to zero. Block rewards will gradually drop until tail emission commences at the end of May 2022. At this point, rewards will be fixed at 0.6 XMR per block.”



Why?

“Miners need an incentive to mine. Because of the dynamic block size, competition between [miners](#) will cause fees to decrease. If mining is not profitable due to a high cost and low reward, miners lose their incentive and will stop mining, reducing the security of the network. Tail emission ensures that a dynamic block size and fee market can develop.”

Monero has a dynamic block reward. When you mine a block, you get a block reward + any transaction fees. The block reward is referred to as a [coinbase transaction](#). The amount in the coinbase transaction is decreasing at a rate of 40% a year, until [tail emission](#) is reached in May 2022, where the block reward will be a constant 0.6 XMR to provide incentive for the miners to continue mining.



[View Full Size Image](#)
[Data Source](#)

[View](#)

Energy Consumption

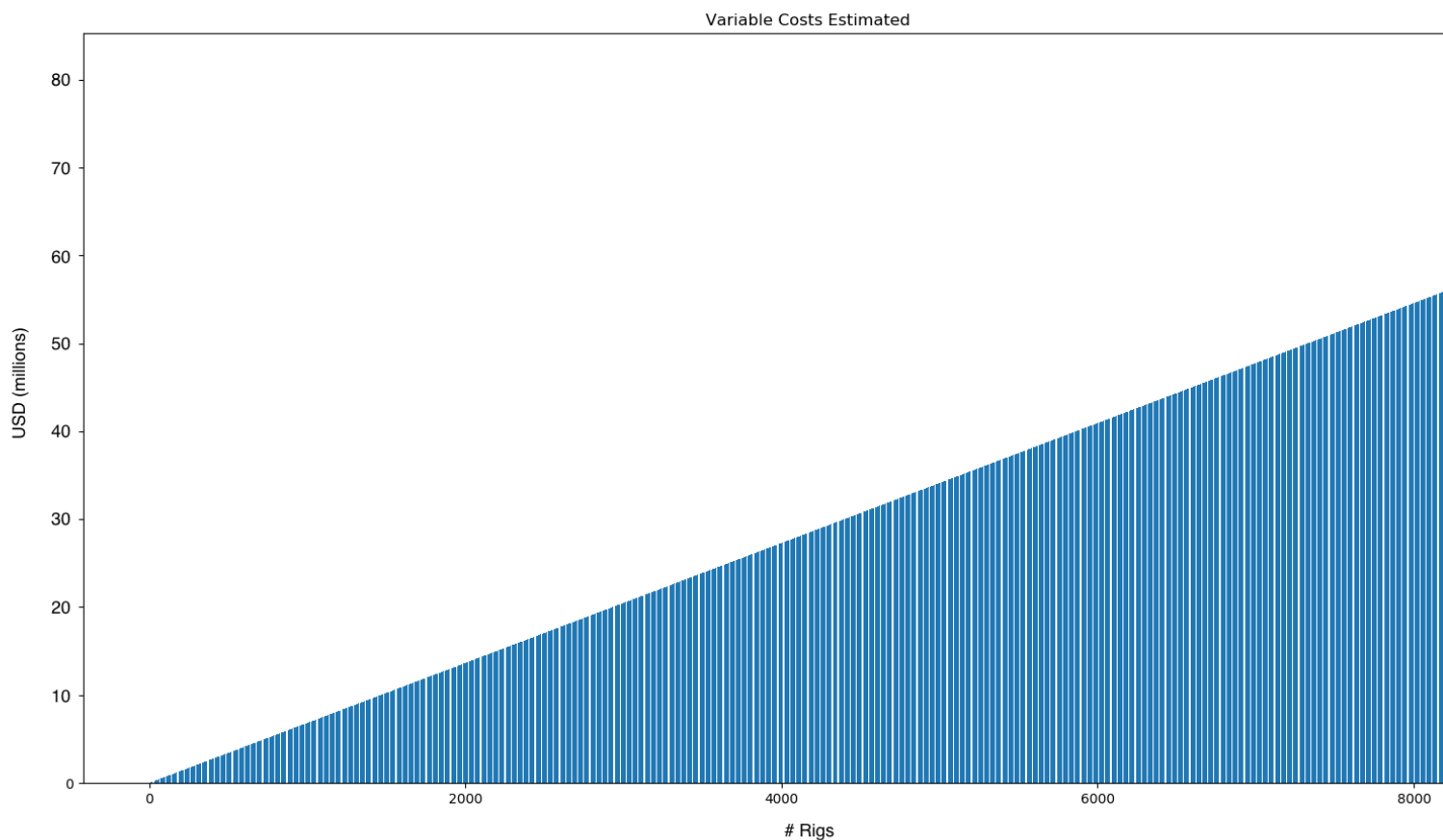
This chart shows the energy consumption in MW/h for mining with anywhere from 1 to 8,334 rigs. Each rig contains 12 GPUs, so this shows 12 to 100,008 GPUs, in multiples of 12. A 90% efficiency AC/DC power conversion for the computer power supplies was used, as shown in the variable costs section above. Each AMD Vega 64 GPU uses 160 watts. The power consumption should remain constant for a five year period, because the mining hardware is best upgraded on a 5 year schedule by depreciating the hardware costs over a 5 year period.

If you take the mean daily revenue for mining Monero (during the first 288 days since release of the GPUs), with a 100,008 AMD Vega 64 GPU mining farm, on a per MW/h scale, the electricity was worth \$560.35 MW/h for up to 18.2 MW/h when allocated to the mining farm during this period.

In five years, the mining profits from mining Monero could be significantly less than they are today because of the tail emission block reward schedule. Transaction fees are always given to miners, which could increase if there is increased adoption of Monero, but for today, they are very small compared to the block reward. Mining Monero in 2019 might be more profitable than expected, because Bitmain was secretly mining Monero with ASICs for most of the second half of 2017 and the first quarter of 2018.

See the actual values in the table below.

# Rigs (multiple of 12 GPUs)	Energy Consumption (MW/h)
1000	2.184
2000	4.368
3000	6.552
4000	8.736
5000	10.92
6000	13.104
7000	15.288
8000	17.472
8334	18.202



[View Full Size Image](#)
[Data Source](#)

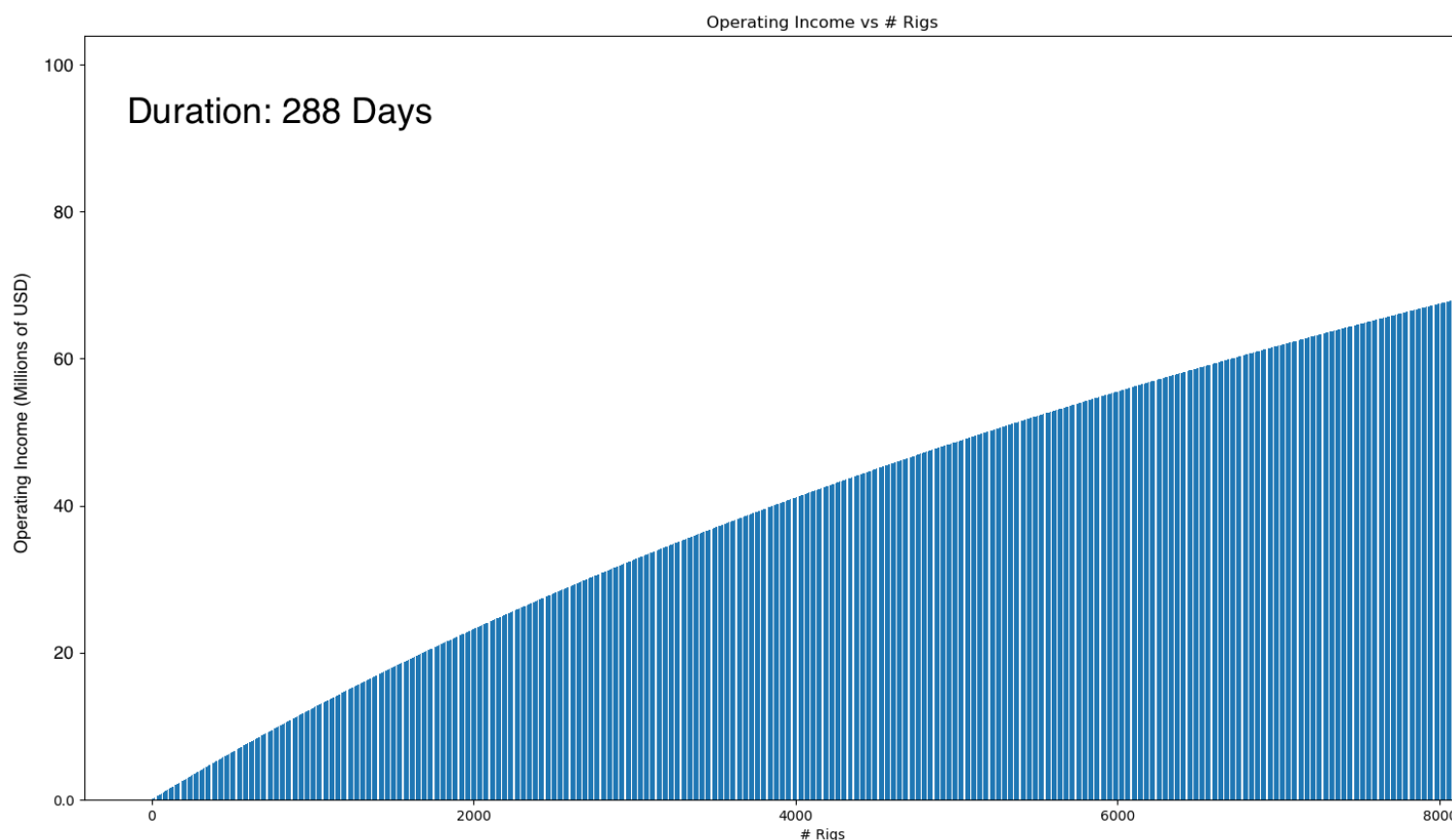
[View](#)

Estimated Variable Costs

This chart shows the estimated variable costs for the mining hardware required to run a mining operation of between 1 and 8334 rigs. The variable costs are estimated because the cost of cooling has not been added. Sales tax has not been included in this figure.

See the estimated variable costs in the table below.

# Rigs (multiple of 12 GPUs)	Cost (Millions of USD)
1000	6.436
2000	12.871
3000	19.307
4000	25.743
5000	32.178
6000	38.614
7000	45.049
8000	51.485
8334 (100,008 GPUs)	53.634



[View Full Size Image](#)
[Data Source](#)

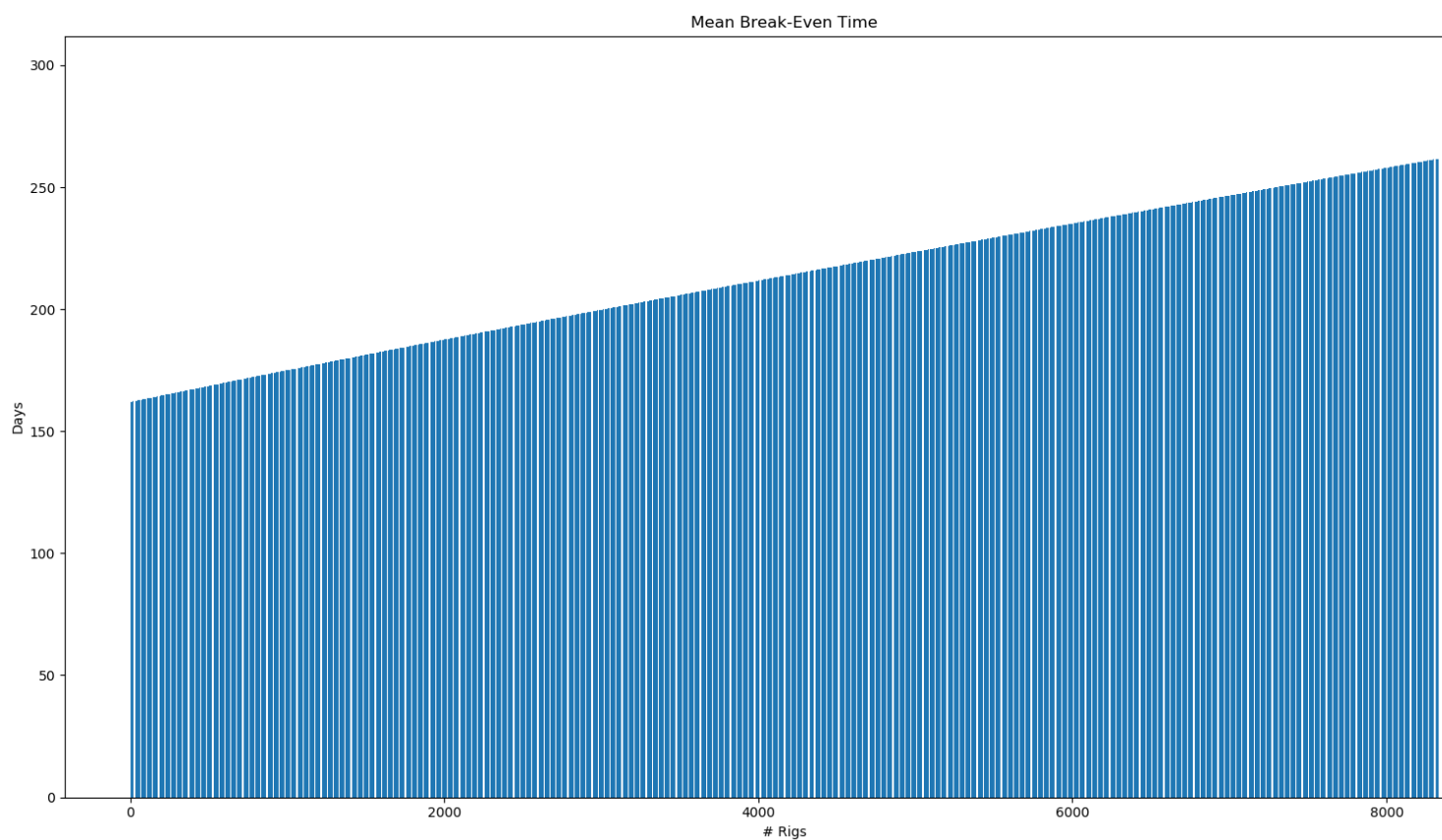
[View](#)

Marginal Operating Income

This chart shows the marginal operating income added by scaling up the number of GPUs. There is decreasing marginal income when adding more GPUs because the block reward for mining Monero is a fixed amount, and the estimated operating income is derived from your share of the total network hashrate. When adding large amounts of hashrate to the network, you no longer exist in a vacuum, and affect the profitability of other miners. In reality, the increased competition may make it unprofitable for competing miners to mine, and their hashrate would be removed from the network.

See the marginal operating income in the table below.

# Rigs (multiple of 12 GPUs)	Operating Income (Millions of USD, 288 days)
1000	12.436
2000	23.206
3000	32.679
4000	41.109
5000	48.681
6000	55.533
7000	61.773
8000	67.485
8334 (100,008 GPUs)	69.288



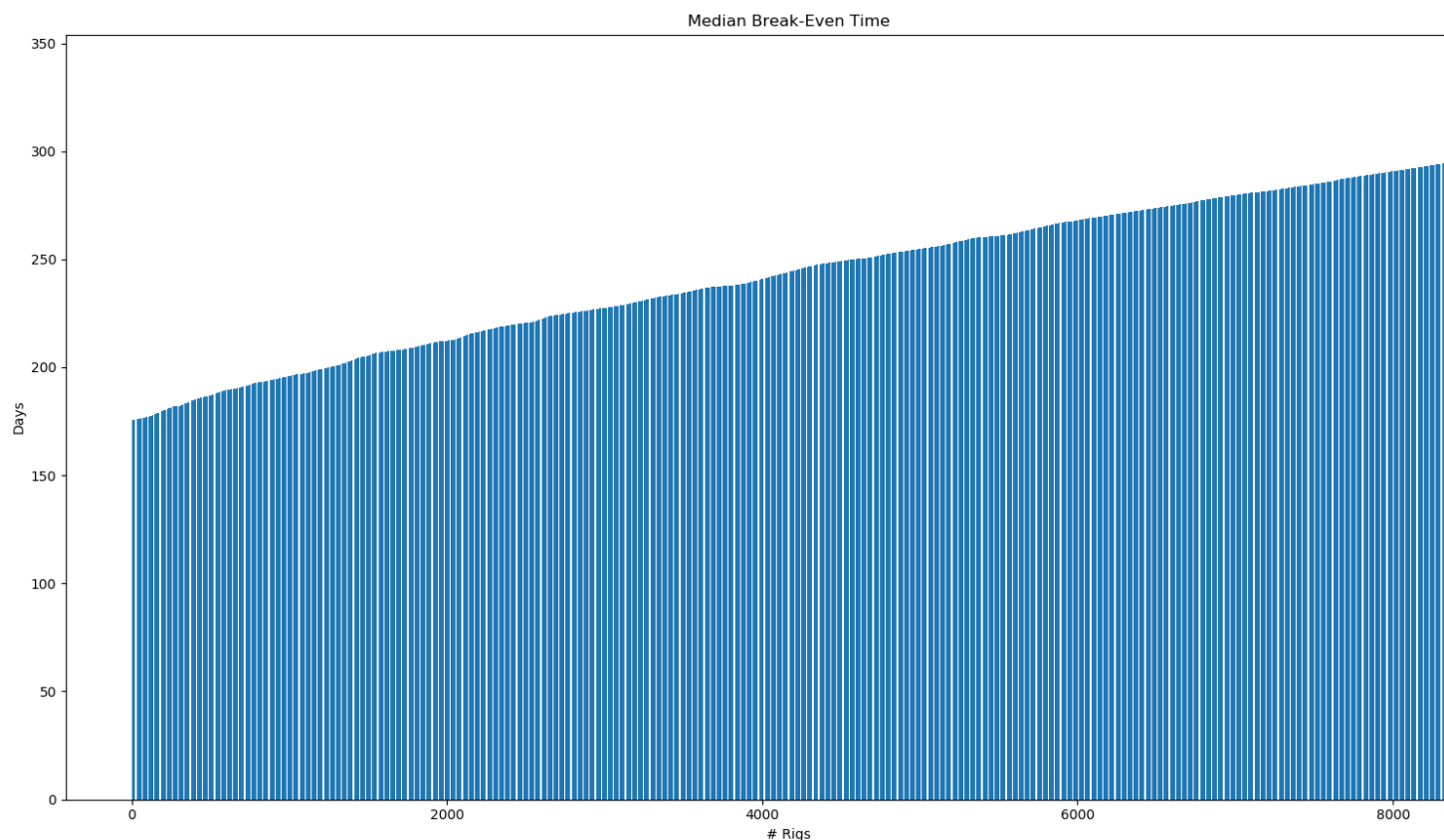
[View Full Size Image](#)
[Data Source](#)

[View](#)

Mean Break-Even Time

Mean break-even time refers to the days until full recovery of hardware costs using the mean daily operating income value for each day during the mining period.

This chart shows the effect the increase in GPUs has on the break even time. The decreasing marginal operating income causes the break even time to increase as the number of GPUs increase. Coal power at a rate of \$18.5 MW/h was used.



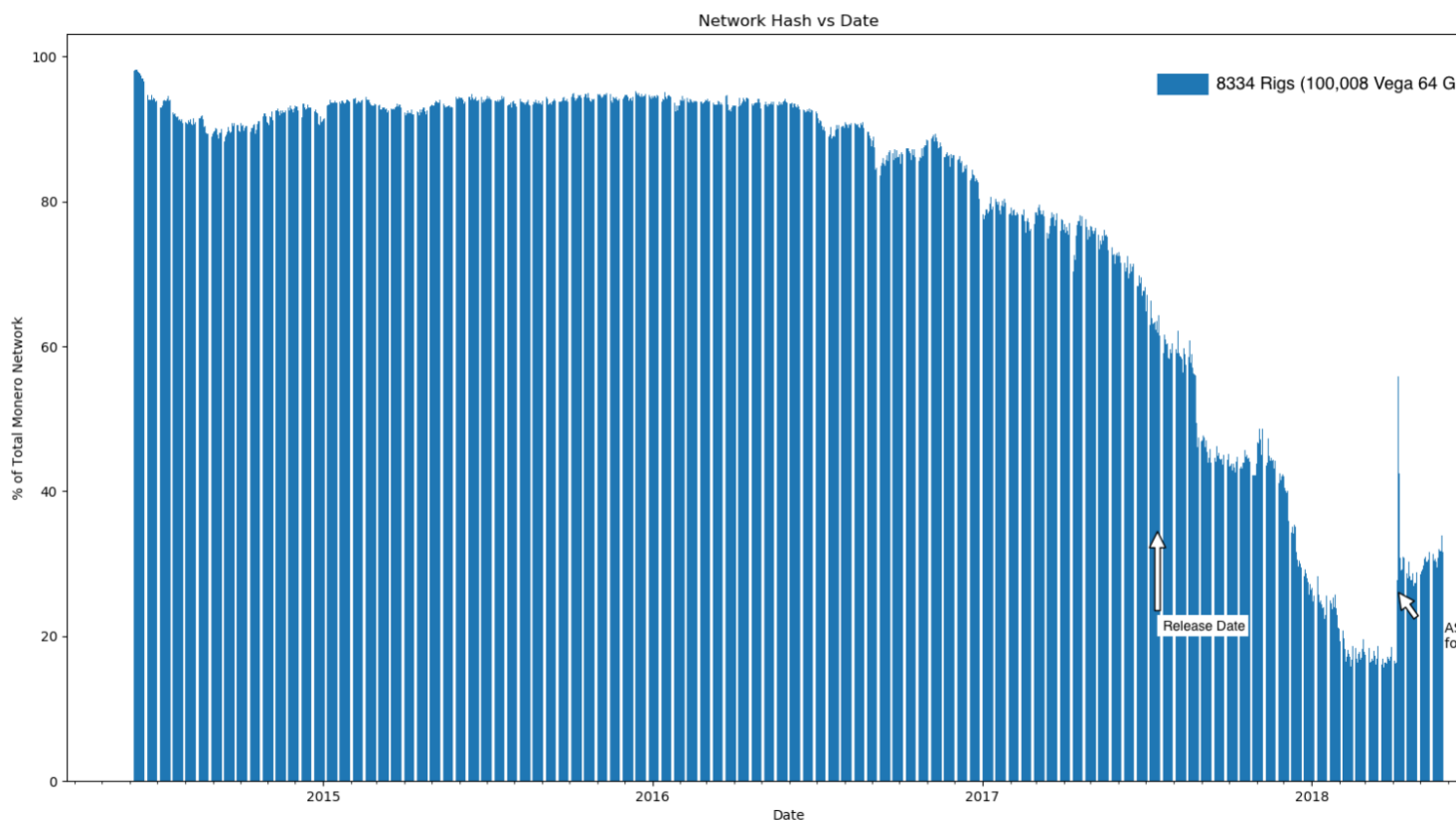
[View Full Size Image](#)
[Data Source](#)

[View](#)

Median Break-Even Time

Median break-even time refers to the days until full recovery of hardware costs using the median daily operating income value for each day during the mining period.

This chart shows the effect the increase in GPUs has on the break even time. The decreasing marginal operating income causes the break even time to increase as the number of GPUs increase. Coal power at a rate of \$18.5 MW/h was used.



[View Full Size Image](#)
[Data Source](#)

[View](#)

Percent of Total Monero Network Hashrate

This graph shows the percentage of the total network hashrate for a mining farm consisting of 8334 rigs (100,008 GPUs). Each AMD Vega 64 GPU is capable of 1990 H/s. At 100,008 GPUs, this would equal a hashrate of 199 MH/s, which is more than double the size of the next largest pool size, [supportXMR](#) at 76 MH/s on July 14th, 2018. Mining pools charge percentage fees, around 1-3%, for smaller miners to be paid consistently for their



hashrate. If this scale is reached, it would be a very good idea to open a mining pool to collect fees from other miners.