An Analysis of Energy and Hardware Impacts on the Bitcoin Mining Network

JAKE LEE, University of Nevada, Las Vegas
YOOHWAN KIM, University of Nevada, Las Vegas

An important part of the bitcoin network is mining, a process of running hash algorithms in order to confirm bitcoin transactions and receive bitcoin rewards. Bitcoin mining is now a major market with multimillion dollar companies developing hardware specifically for bitcoin mining. By analyzing bitcoin income, hardware costs, and electricity costs in the past 15 months, we were able to determine that miners have reached negative net income due to injection of capital into the system as well as reinvestment of income. This indicates that miners will not be able to continue hardware investment without additional capital, suggesting a slower hashrate growth in the future. We then discuss a amplifying oscillation behavior upon reaching a mining equilibrium, in which operating costs equal income, as well as potential exploitation due to industrial mining centralization.

Categories and Subject Descriptors: C.3 [**Computer-Communication Networks**]: Special-Purpose and Application-Based Systems — Economics

ACM Reference Format:
ACM Trans. Econ. Comp. V, N, Article A (January YYYY), 20 pages.
DOI: http://dx.doi.org/10.1145/0000000.0000000

1. INTRODUCTION

Bitcoin is a cryptocurrency introduced in 2008. It was designed as an "electronic cash system" that doesn't require a central authority by using a peer-to-peer network [Nakamoto 2008]. It has gained popularity in the last few years, and it is now being accepted by several major companies, including Overstock, Expedia, and Dell [Ember 2014].

In order to use bitcoin, each user must have a wallet. A wallet consists of a client that manages a public key and a private key; the public key is the address used to accept bitcoins for that wallet, and the private key is required in order to send bitcoins from that wallet. The balances are managed by a network-wide system called the blockchain, represented in Fig. 1.

When a transaction occurs, the transaction is given an ID (often referred to as TXID) and the information concerning the transaction is sent to a transaction cloud. Bitcoin miners, groups or individuals running the Bitcoin mining software, then choose transactions from the cloud and form them into blocks. These miners then run random hash algorithms, which reform data into a unique string of numbers and letters. When a miner is able to calculate a hash that meet certain criteria, the block of that miner is added onto the blockchain [Peck 2013]. The balance of each address is calculated by considering all relevant transactions in the blockchain. Delays in information propagation can cause a branch to form in the blockchain, in which two blockchains are formed due to blocks being added at the same time. In this case, the chain to which the next

DOI: http://dx.doi.org/10.1145/0000000.0000000

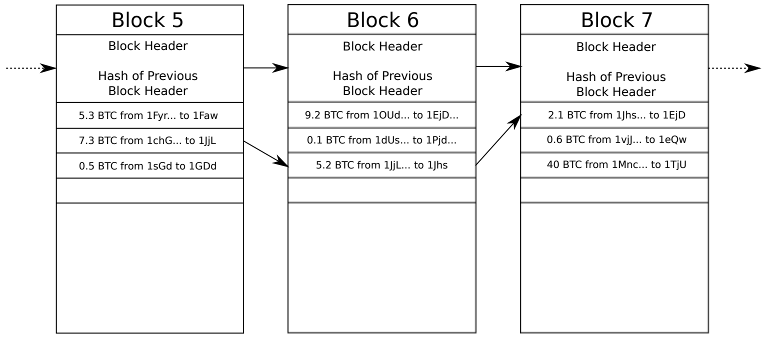


Fig. 1. A simplified diagram describing the blockchain system. [Bitcoin.org 2014]

block is added to is chosen as the main chain, and the other chain is ignored [Decker and Wattenhofer 2013]. This entire process is called Proof of Work, and it gives the transaction process a concept of time and order.

The main aspect of the bitcoin process that the paper will focus on is the mining process. The hash algorithm that Bitcoin uses is SHA-256, but other cryptocurrencies have used other algorithms such as Scrypt. Miners originally used CPUs in order to mine (hence the references to CPU power in the original Nakamoto paper [Nakamoto 2008]), but miners have since moved to GPUs, FPGAs (Field Programmable Gate Arrays), and ultimately ASICs (Application Specific Integrated Circuits). Each step in hardware development significantly lowered hardware costs and increased efficiency. Although the miners main purpose in the network is to confirm transactions, most miners mine for the mining rewards. Every time a miner is able to add a block to the blockchain, the miner is rewarded a certain amount of bitcoins. This reward serves two purposes: to provide an incentive to continue confirming transactions and to create new bitcoins in the system. The network regulates itself so that a reward is given every 10 minutes by adjusting the difficulty of mining every 2 weeks in accordance with the total network hashrate - higher the hashrate, higher the difficulty. This balance is shown in Fig. 3(b). The system can be compared to a lottery given every 10 minutes: as more people sign up for the lottery, the difficulty of getting the reward increases. The reward for mining is halved every 4 years, and only 21 million bitcoins can ever be mined [Bitcoin.org 2014].

Due to the ever-increasing difficulty of mining, miners with small computing power (often measured in gigahashes per second and referred to as “hashrate”) will often join “pools” in order to mine as a group. If a block is found by any member in the group, The rewards are split between all of the members. Major portions of the total mining hashrate are consisted of pools, and the current hashrate distribution among pools is shown in Fig. 2.

This paper seeks to analyze the past 15 months of the bitcoin mining network and discuss the current trend in the mining market. It seeks to gain a more clear understanding into the explosive growth in hashrate observed in the past, and attempts to predict mining behavior in the future. Section 3 will discuss the players of the mining market and their impacts upon it. Section 4 will analyze historical data and attempt to understand the past trends, and section 5 will use those trends to describe trends in the future. Section 5 also presents a new behavior due to a mining equilibrium.

2. RELATED WORKS

The first documentation for Bitcoin was Satoshi Nakamoto’s whitepaper, which described the basic mechanics of the currency [Nakamoto 2008]. Since then, various lit-

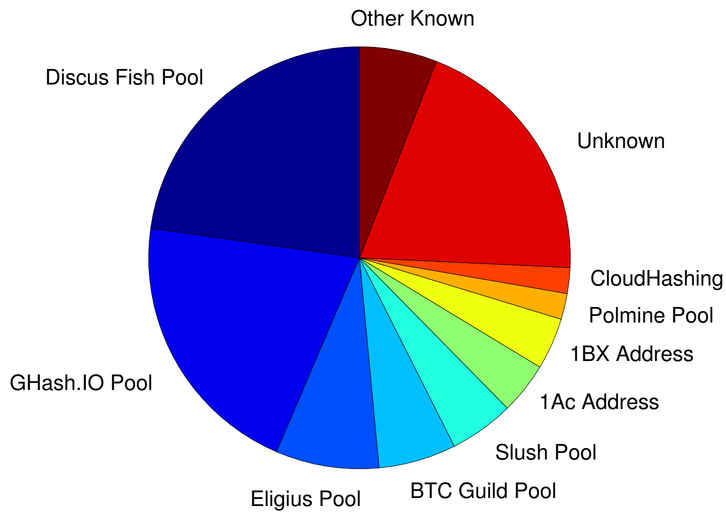


Fig. 2. Total Hashrate Distribution among Mining Pools in July, 2014. [Blockchain 2014c]

erature have discussed the economic, social, and technological impacts of Bitcoin on the status quo. Additionally, several whitepapers have been written to present alternate currencies that modify bitcoins in order to improve various aspects. For example, Proof of Stake was presented by Daniel Larimer in order to replace the Proof of Work system implemented in Bitcoin [Larimer 2013]. Although an attempt at estimating bitcoin energy use was made by the blockchain organization, an inaccurate assumption made during the calculations caused the result to be highly unrealistic. To our knowledge, no previous academic attempts have been made to analyze both the costs and revenue of bitcoin mining by compiling historical data.

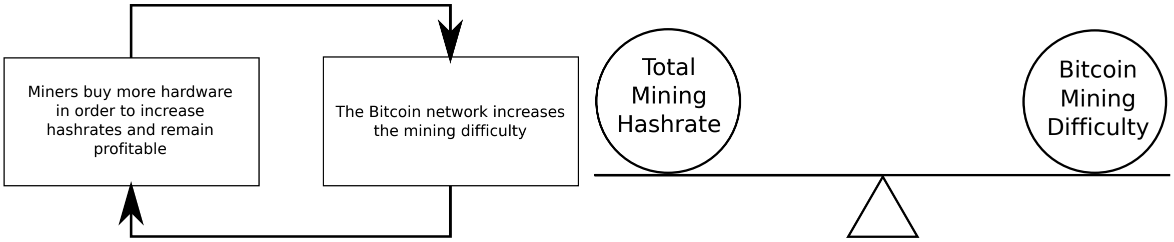
3. THE PLAYERS IN THE MINING MARKET

3.1. The Miner

A Bitcoin miner can be described as a group or individual that is running the Bitcoin mining software in order to secure transactions. However, the vast majority of miners are not mining for the sole benefit of the Bitcoin network. Most miners, including the miners with the highest hashrates, are mining in order to make a profit from mining rewards [Reuters 2013]. In order to make a profit, several conditions must be met:

— The mining rewards must be able to cover the initial hardware cost within a limited period of time.
— The operational cost for a period of time must not be higher than the mining rewards during that time.
— Bitcoin must remain valuable.

These conditions may be difficult to achieve due to several factors working against the bitcoin miner. The rising difficulty due to competition between miners is the main obstacle to achieving profitability, as it continuously diminishes the mining rewards that the miner receives. Additionally, the mining rewards are cut in half every four



(a) (b)

Fig. 3. The balance between hashrate and difficulty in bitcoin mining

years, prohibiting long term returns. Therefore, the miner must rely on a few methods in order to ensure that a break-even point, or a return on investment, can be reached. First, the miner must buy the most efficient miner for the lowest price possible. This ensures that the initial investment cost and the electricity cost cause minimal impact to the net profits of the miner. Second, a miner may assume some risk by keeping its earnings in Bitcoin and hoping for an increase in value. A price increase in bitcoin may be the quickest way to gain profitability, but there is also a risk of a price decrease, which would also decrease profitability. Finally, the miner must assume one of two strategies:

— Short Term: The miner starts with a set amount of hardware, mining until the operational costs are higher than the rewards. The miners are then sold off at a very low price, possibly resulting in a net profit.
— Long Term: The miner starts with a set amount of hardware, and continues buying more hardware with the earnings in order to keep up with the difficulty. Stronger and more efficient hardware is continuously bought.

The short term plan does not require a large initial investment; however, it may be harder to reach profitability. The long term plan may be easier to reach profitability with, but requires a very large initial investment (often tens of thousands of dollars) and early adoption of high-end hardware. The majority of the total hashrate comes from miners employing the long term plan (as they are continuously increasing their hashrate). As the total network hashrate increases due to long term miners, the difficulty increases, resulting in a cycle shown in Fig. 3(a) and a miner hardware arms race between miners.

3.2. The Hardware Producer

Initially, bitcoin mining was done through the use of consumer CPUs and GPUs. However, with the development of mining-specific Field-programmable Gate Arrays (FPGAs) and Application Specific Integrated Circuits (ASICs), small companies began developing and selling these mining hardware products to miners. ASIC mining hardware is now a huge market with several multimillion dollar companies dedicated to the development of mining hardware. KnCMiner, one of these companies, sold 8 million dollars of its newest mining ASIC hardware within 24 hours [Wile 2013], and BitFury, another mining hardware company, raised 20 million dollars in funding from various investors [Rizzo 2014a]. The competition between companies is pushing technology development, as shown by KnCMiners announcement of 20nm mining chips in March, 2014 [Hajdarbegovic 2014c].

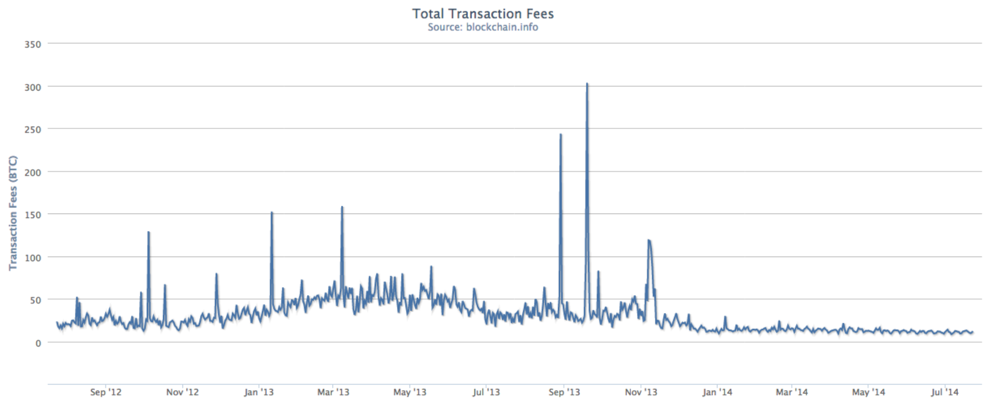


Fig. 4. The significant decrease in total transaction fee per day in early 2014 [Blockchain 2014e]

4. ELEMENTS OF MINING ECONOMICS

This section discusses several factors that can affect a miners net profits. By analyzing the total network hashrate of Bitcoin and historical hardware data, it is possible to calculate the overall mining rewards, hardware cost, and electricity cost.

4.1. Mining Rewards

4.1.1. Overview. Currently, when a miner solves a block, 25 bitcoins are awarded. This is estimated to occur every 10 minutes, and adjustments are made for faster total hashrates by increasing the network difficulty (or lowering the difficulty in case of a slower total hashrate). This process is described in Fig. 3. Note that 10 minutes is just an average - it can take a few seconds or several hours in order to find the next block.

The number of bitcoins awarded is halved every 4 years, and the next halving is estimated to be in 2016. Therefore, miners must expect rewards to be halved sometime in 2016, unless bitcoin prices double before the halving. Bitcoin rewards are reliant on bitcoin prices relative to fiat currencies, such as the US Dollar or the Chinese Yuan, as miners must convert the bitcoins into these currencies in order to pay for hardware (some companies accept bitcoin as payment) and electricity.

Miners also receive rewards in forms of transaction fees. When bitcoins are transferred, users can choose to add a small fee to the transaction in order to support the miners. In the past, a minimum transaction fee was required for small transactions. However, this was decreased significantly in early 2014 due to the high prices of bitcoin [Bradbury 2014], and the decrease in total transaction fee is visible in Fig. 4.

A study published in The International Conference on Digital Security and Forensics suggests that these near-zero fees for transactions are unsustainable for the Bitcoin network in the future, as transaction fees ultimately need to offset increasing miner costs and decreasing mining rewards [Kaskaloglu 2014].

4.1.2. Historical Trends. The total mining rewards were calculated by using two different methods.

First, total mining rewards were taken from collected Bitcoin data. The Blockchain organization tracks all blocks, transaction fees, and bitcoin price in real time and provides a database of total miner revenue per day in USD. This graph is shown in Fig. 5.

The daily mining revenues were then summed up for each month from April 2013 to June 2014.

Fig. 5. Miner revenue per day in USD for the last 2 years [Blockchain 2014d]

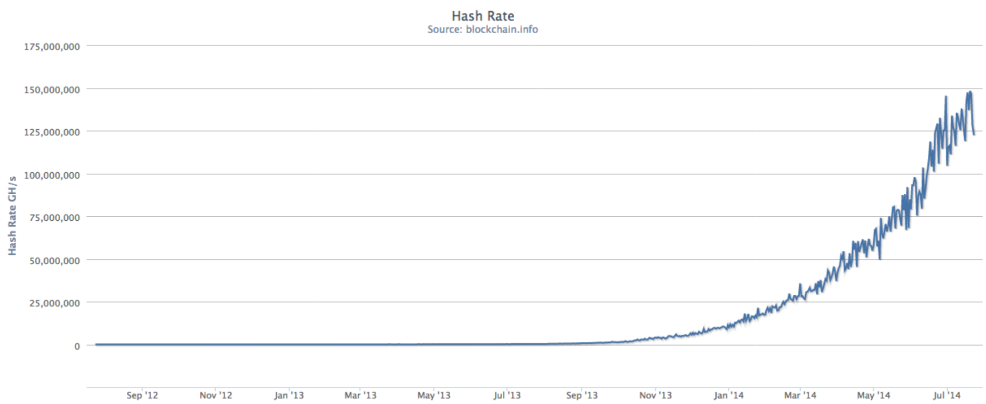


Fig. 6. Total network hashrate per day in Ghash/second for the last 2 years [Blockchain 2014b]

Second, total mining rewards were calculated theoretically. The Blockchain organization also provides an estimate for the total hashrate of the entire bitcoin network for each day, as well as the difficulty for that day. The graphs for the total network hashrate and difficulty are shown in Fig. 6 and Fig. 7, respectively.

With the hashrate and difficulty, it is possible to estimate the average time between blocks finds with (1).

$$t_b = \frac{\text{difficulty} * 2^{32}}{\text{hashrate}} \tag{1}$$

where t_b is the time between block finds in seconds. This should be close to 10 minutes.

It is now possible to find the average number of blocks found in each month. By adding the average transaction fee for each month from April 2013 to June 2014 (400 BTC according to Fig. 4) and multiplying it by a constant price for bitcoin (620 USD was used), it is possible to calculate the theoretical income for miners in USD, assuming that the bitcoin price remained constant. This gives an insight into how much the bitcoin price can affect the income for Bitcoin miners.

The results from both methods are shown in Fig. 8

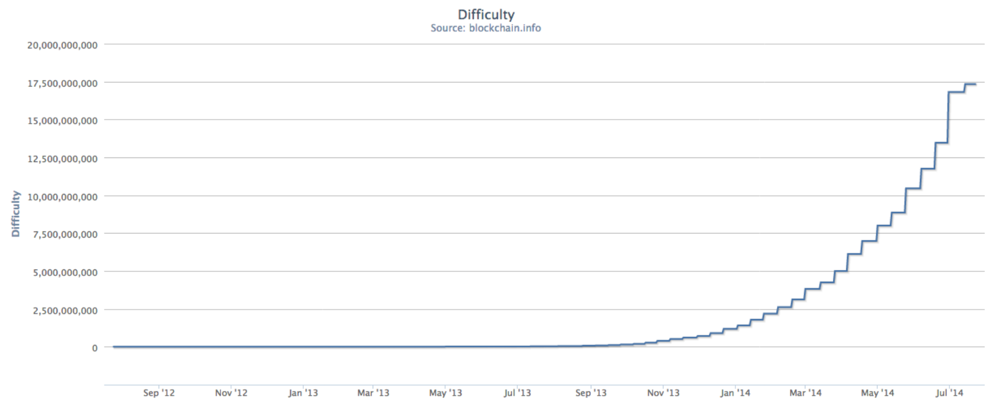


Fig. 7. Mining difficulty per day for the last 2 years [Blockchain 2014a]

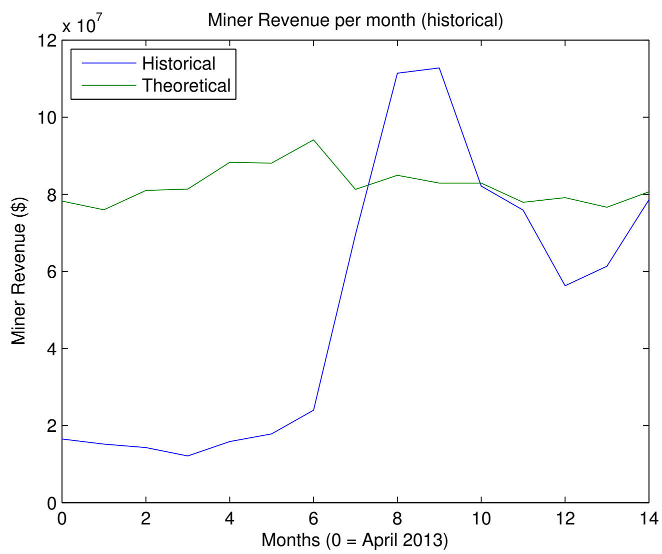


Fig. 8. Historical and theoretical miner revenue from April 2013 to June 2014.

While the theoretical miner revenue remained constant for 15 months (due to the controlled bitcoin reward rate at 25 bitcoins every 10 minutes), the volatile price of bitcoin caused big variations in the historical miner revenues for each month. This emphasizes the importance of the bitcoin market value in profiting by mining.

Note that we are assuming all mined bitcoins are immediately converted to fiat currency in order to calculate revenue; if miners held on to bitcoins, fiat revenue may be higher or lower.

4.2. Hardware Costs

4.2.1. Overview. A major part of a miners total costs come from hardware purchases. In order to start mining, the miner must initially buy mining hardware. Mining hardware can be very expensive, with some ASIC miners reaching up to tens of thousands of dollars. Therefore, it is important that the mining hardware eventually pays for it-

Table I. ASIC hardware cost data. (The hardware is released if it is available to customers)

Date Released	Name	Perf. (Gh/s)	Price ($)	Value ($/Gh/s)	Source
Jan. 2013	Avalon 1	66	1299	19.68	[BitSyncom 2012]
Aug. 2013	KnC Jupiter	400	4995	12.49	[Spaven 2013; KnCMiner 2013]
Nov. 2013	AntMiner S1	100	299	2.99	[Antminer 2013; BITMAIN 2013]
Jan. 2014	Avalon 2	105	200	1.90	[Avalon 2014a]
Apr. 2014	Antminer S2	1000	3899	3.90	[Antminer 2014a]
Apr. 2014	Avalon 3	325	480	1.48	[Avalon 2014c]
Apr. 2014	Avalon 3 2U	890	1800	2.02	[Avalon 2014b]
Jun. 2014	Antminer S3	478	450	0.94	[Antminer 2014b]
Jul. 2014	Prospero X-1	100	415	4.15	[BlackArrow 2014b; BlackArrow 2014a]

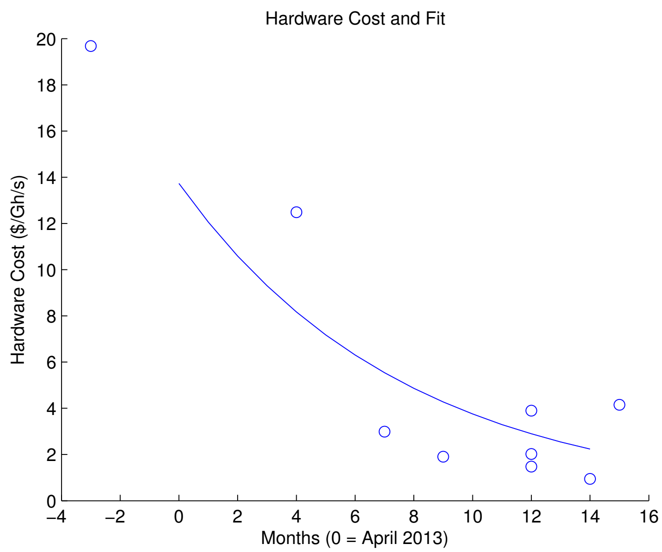


Fig. 9. Historical mining hardware value data and its fit.

self. However, this can be a large gamble due to the volatility of the bitcoin price and the rising difficulty. Miners must always buy the hardware with the lowest cost per Gh/s to increase their chances of recovering the hardware cost as quickly as possible.

4.2.2. Historical Trends. Due to competition between hardware companies, the cost per Gh/s for ASICs has gone down throughout the last two years. In order to model this decrease, data was collected for several ASICs over the past two years. This data is shown in Table I and Fig. 9. (2) was found to describe the trend expressed in the data.

Note that data for GPUs and FPGAs were not collected due to variation in performance and cost and lack of documentation. It can also be assumed that the development of ASICs made GPUs and FPGAs obsolete by pushing the difficulty beyond their profitability point, ending their operation.

$$V_h = 13.73e^{0.1297t} \tag{2}$$

where V_h is the hardware value in USD per gigahash per second and t is the number of months after April 2013.

By using the hashrate data shown in Fig. 6, it is possible to calculate the hashrate increase per month. By assuming that the miners will always buy the highest value

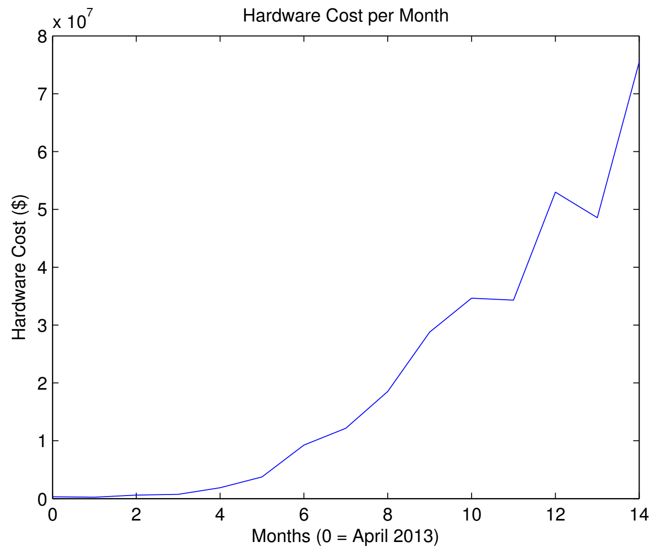


Fig. 10. Historical mining hardware cost per month data over 15 months assuming ideal conditions.

(lowest \$/Gh/s) hardware, the amount of money spent on hardware each month can be calculated with (3).

$$C_h = \Delta\text{hashrate} * V_h \tag{3}$$

The results of these calculations are shown in Fig. 10.

Hardware cost per month has increased dramatically in the past 15 months. The hardware cost for June was approximately 75.5 million dollars, and a continuation of this trend would result in over a hundred million dollars spent per month total for acquiring hardware. Compared to the miner revenue shown in Fig. 8, hardware cost seems to take a huge chunk out of the income. This is in accordance with the long term plan presented in section 3.1, in which most of the income is used in order to buy additional hardware.

4.3. Electricity Costs

4.3.1. Overview. A major part of the operating cost is the electricity costs of running the hardware. This cost will often determine the profitability of the mining hardware, as the hardware must be able to earn more money than it uses. Energy efficiency is seen on two levels: chip efficiency and hardware efficiency. While developing ASIC chips can be resource intensive, many hardware manufacturers are taking other companies' chips and attempting to improve efficiency and performance through hardware design.

The energy used in bitcoin mining is becoming a big concern, especially with the increasing global hashrate. KnCMiner has built a 10-megawatt datacenter in Sweden for bitcoin miner hosting [Miller 2014a], and there are plans for a 50-megawatt datacenter by a California-based company, Aquifer [Miller 2014b]. While these may seem small compared to some 100-megawatt datacenters built by major corporations [Fehrenbacher 2012], bitcoin mining energy use is expected to continue its increase, potentially placing bitcoin mining as a significant energy consumer in the IT energy market.

Table II. ASIC hardware efficiency data. (The hardware is released if it is available to customers)

Date Released	Name	Perf. (Gh/s)	Power (W)	Eff. (W/Gh/s)	Source
Jan. 2013	Avalon 1	66	400	6.06	[BitSyncom 2012]
Apr. 2013	Sapphire	0.336	2.55	7.59	[Friedcat 2013]
Jun. 2013	Jalapeno	5	30	6	[BFL 2013]
Aug. 2013	KnC Jupiter	400	600	1.5	[KnCMiner 2013]
Nov. 2013	Antminer S1	100	200	2	[Antminer 2013; BITMAIN 2013]
Jan. 2014	Avalon 2	105	340	3.23	[Avalon 2014a]
Apr. 2014	Antminer S2	1000	1100	1.1	[Antminer 2014a]
Apr. 2014	Avalon 3	325	405	1.25	[Avalon 2014c]
Apr. 2014	Avalon 3 2U	890	1037	1.17	[Avalon 2014b]
Jun. 2014	Antminer S3	478	366	0.77	[Antminer 2014b]
Jul. 2014	Prospero X-1	100	75	0.75	[BlackArrow 2014b; BlackArrow 2014a]

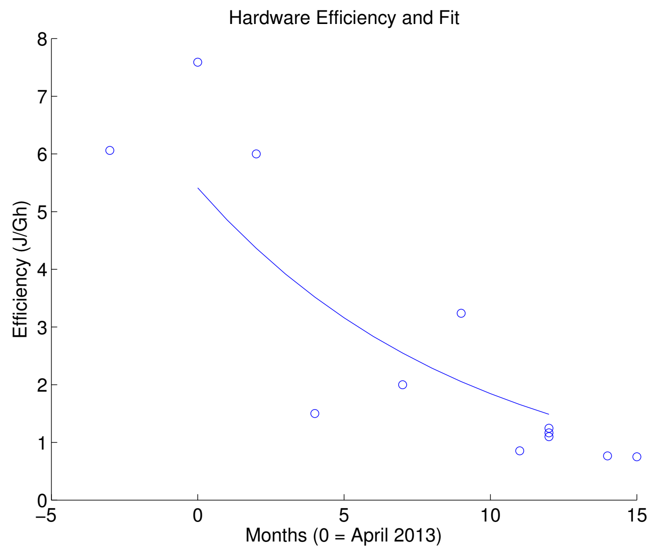


Fig. 11. Historical mining hardware efficiency data and its fit.

4.3.2. Historical Trends. In order to understand the energy use of bitcoin mining, the efficiency of bitcoin miners must be considered. Historical data was collected for 11 ASIC miners, and is shown in Table II and Fig. 11. (4) was found to fit the trend described by the data. Note that there is more data due to better documentation; hardware price are more variable and more subject to change.

$$E_h = 5.412e^{0.1076t} \tag{4}$$

where E_h is the hardware efficiency in watts per gigahash or joules per gigahash per second and t is the number of months after April 2013.

By using the average hashrate per month given in Fig. 6, it is possible to calculate the number of hashes calculated per month. By multiplying this by the efficiency, the amount of joules used per month for bitcoin mining can be calculated. This value has been converted to KWh in order to facilitate price calculations, and is displayed in Fig. 12.

The data shows that during the month of June 2014, the bitcoin mining network used 93.1 gigawatt-hours of electricity. This is small (about 0.12%) compared to the av-

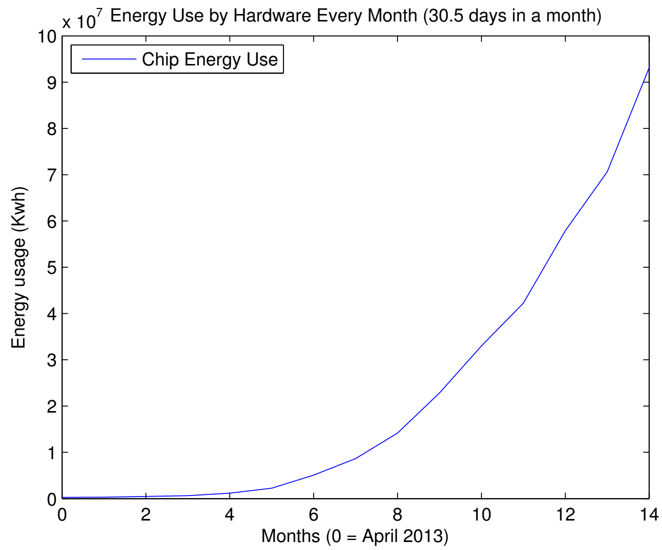


Fig. 12. Historical mining energy use data over 15 months assuming ideal conditions.

Table III. Electricity Usage/Generation of Various Entities Compared with Bitcoin Mining

Entity	Elec Usage per Month (GWh)
Average American House Monthly (2012)	0.0000903 [USEIA 2014b]
Bitcoin Mining Monthly(June 2014)	**93.1**
Google Monthly (2010)	188.3 [Google 2011]
Average US Nuclear Plant Monthly (2012)	983.3 [USEIA 2013]
Los Angeles County Monthly (2011)	5773 [ECDMS 2014]

erage of 77.5 terawatt-hours of electricity used by the information and communication technologies sector per month [Lannoo et al. 2013], but note that the value calculated above does not include the computers, monitors, internet services, cooling systems, and other operating energy costs. The actual value may be higher. Further comparison of electricity usage with other entities are shown in Table III.

In order to calculate the electricity cost, the average price for electricity is needed. In this case, the average electricity price of 10.18 cents per kilowatt-hour for the United States from 2013 to 2014 was used [USEIA 2014a]. Table IV presents the average electricity prices for various other countries. Figure 13 shows the result of these calculations.

The results show that every month, millions of dollars are spent in electricity costs to mine bitcoins. In June 2014, miners spent approximately 9.48 million dollars in electricity costs. This is in stark contrast to a previous calculation presented in a Forbes article, which suggested that Bitcoin mining spent 15 million dollars in electricity every day, resulting in about 460 million dollars each month [Worstall 2013]. It must be noted that this article assumed a electricity usage of 650 watts per gigahash, while we derived a value closer to 5 watts per gigahash from our data. Additionally, the maximum revenue possible per month is theoretically 110000 BTC, or 65 million USD. It is unrealistic to suggest that the operational electricity costs are nearly seven times the total income. Our calculated value may be lower than the actual value, as we are assuming that all miners are using the most efficient hardware available and are ex-

Table IV. Electricity Prices for Various Countries in 2010. Tax not included. [Agency 2012]

Country	Industry Price (USD/KWh)	Household Price (USD/KWh)
Canada	0.0601	0.0822
France	0.0964	0.1216
Germany	0.1062	0.1838
Italy	0.2010	0.1964
Japan	0.1223	0.1856
Mexico	0.1071	0.1784
Spain	0.1266	0.2007
Sweden	0.1005	0.1438
United Kingdom	0.1263	0.1895
United States	0.0679	0.1158

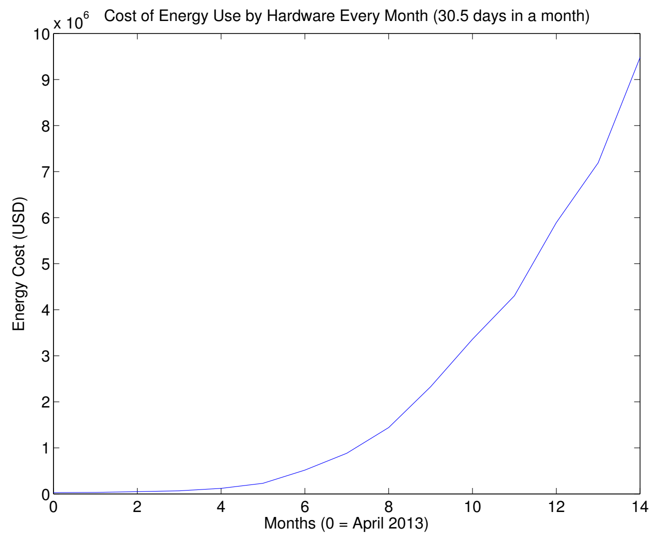


Fig. 13. Historical mining energy cost data over 15 months assuming ideal conditions.

cluding energy usage related to cooling, bandwidth, and other operations. However, we are confident that our calculations are more realistic representations of the energy use of bitcoin, as it allows for net revenue above operational costs.

Electricity costs are the defining factor of the profitability of mining, and those with the most efficient mining hardware will always be at a significant advantage over others with less efficient hardware. Electricity costs will only continue to increase unless significantly more efficient mining methods are found or cheaper sources of electricity are developed.

4.4. Net Miner Earnings

By combining the data from sections 4.1.2, 4.3.2, and 4.2.2, the net profit of the entire miner network can be calculated for every month. The calculated net profits are shown in Fig. 14.

Figure 14 shows that net miner profits have fallen significantly for the past 15 months, dipping below zero in April 2014. Considering that these calculations were performed assuming ideal conditions, in which every miner always has the most effi-

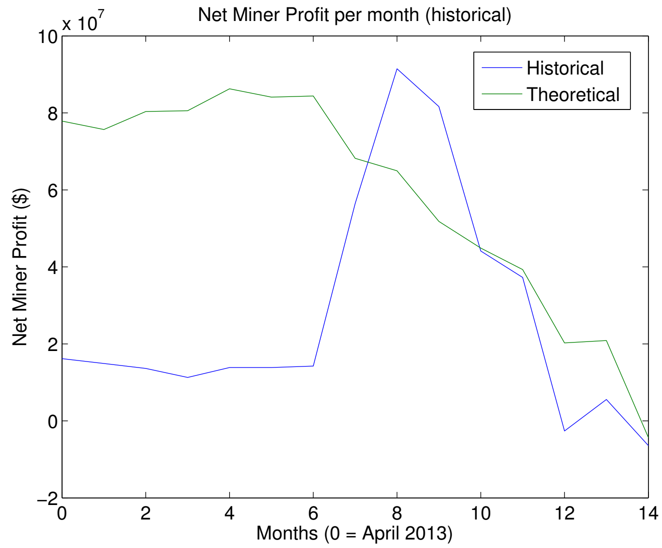


Fig. 14. Net profit from mining over 15 months assuming ideal conditions.

cient and high-value hardware, it is possible to suggest that in reality, net miner profits have fallen below zero earlier in the year.

There are several ways to explain why mining has continued even after net miner profits have fallen below zero. First, many miners may not have reached an ROI (Return on Investment) on their investment on bitcoin hardware yet. These miners may continue mining until electricity costs and diminishing returns prohibit continued operation, but these miners are still at a net loss. Additionally, industrial miners employing the long term strategy described in section 3.1 are continuing to reinvest income and additional capital into buying more hardware, resulting in a small or negative net profit. It must be noted that an increased bitcoin price is essential to the investment plans of many mining companies. As seen in Fig. 8, market value strongly influences the income of miners. George Bachiashvili, CEO of the Georgia Co-Investment Fund, which invested in the mining company BitFury, suggests that “If it rises and reaches several thousand per bitcoin, I think good revenue can be generated” [Rizzo 2014b].

5. FUTURE PROJECTIONS

5.1. Mining Hardware Projection

Hardware is expected to follow the current trend of increasing efficiency. However, the increase rate of efficiency and value is not expected to match the increase in hashrate. In fact, the development rate (if the current trend continues) is expected to slow down as ASIC development catches up to current limits of technology. KnCMiner has already developed a 20nm ASIC chip [Hajdarbegovic 2014c], and unless signifcant developments are made in chip design or production size, efficiency improvement is expected to slow down. It is suggested that bitcoin mining hardware may follow the trend described by Koomey’s Law, in which computing efficiency doubles every 1.5 years [Koomey et al. 2011]. A new company, CoinBau AG, is already claiming that it can produce a mining chip that will halve energy usage [Drner 2014].

The value of ASIC miners, however, is expected to increase in the future due to competition between companies. Companies will continue to offer higher hashrates for lower prices in order to stay competitive. However, the consumer mining market seems to be shifting. Due to rising entry points for consumers, mining companies are now offering hosting solutions for mining machines. KnCs 10 gigawatt datacenter was built for this purpose [Miller 2014a], and BitFury is offering hosting solutions for customers as well [Hajdarbegovic 2014b]. The cloud/hosted mining platform benefits both consumers and hardware companies. Consumers benefit because hosted mining removes operation obligations (shipping, electricity, cooling, noise, internet, etc.) albeit for a hosting fee. Hardware companies also benefit because they can keep the hardware that they produce mining at their own location, removing packaging, shipping, and other logistical costs. CEX.io, a cloud mining service, provides a unique service in which customers can buy and sell Gigahashes of mining on a free market [Hajdarbegovic 2014a]. This means that customers can potentially profit from the mining itself as well as from trading on the market. The historical prices for 1 Gh/s from CEX.io are shown in Fig. 15.

However, this shift to hosted mining creates an issue of mining centralization. It was mentioned in section 1 that miners often form a pool, a distributed computing network, in order to combine computing power. On June 2014, Ghash.io, a pool in which CEX.io (the cloud mining service) mines, reached 50% of the total network mining rate [Shanafelt 2014]. This is significant, as controlling 51% of the hashrate could potentially allow for bitcoin blockchain manipulation, allowing for double spends. Double spends, or 51% attacks, are exploits in which bitcoin is spent twice by controlling the blockchain process with a superior mining rate. This method of attack was predicted as a potential exploit in the original bitcoin whitepaper, which states, “The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.” [Nakamoto 2008]. While ghash.io has promised to restrict its hashpower to 40% of the network [Wilhelm 2014], the increasing industrial centralization of bitcoin mining may still increase chances of a 51% attack occuring. Some argue that the attack is still highly unlikely, however, as such an attack would significantly decrease trust in the system, resulting in a crash in bitcoin price. The attacker would lose money in the process, making the attack itself unviable [Hern 2014].

5.2. Hashrate Projection

As shown in Fig. 6, the total network hashrate has grown significantly in the past. However, as shown in Fig. 14, net miner revenue has decreased dramatically due to hardware costs and electricity costs. Under ideal conditions described in section 4, the miners are currently making negative profit each month.

When miner profits are below zero, it indicates that miners are now using external capital in order to buy more hardware. This should result in a slower hashrate growth, as less miners are able to buy more hardware. This should be mirrored in the difficulty growth. July’s difficulty increase of only 3% (The lowest since early 2012) may be a result of the decreasing net miner profit. However, it is also suggested that this may be caused by the operation of new mining hardware (the antminer S3) spiking the difficulty in June [CoinGazette 2014].

5.3. Mining Equilibrium

The relationship between costs, income, hashrate, and difficulty brings up an interesting question. Can an equilibrium be reached where the income of the miner and the operating costs reach an equilibrium?

The equilibrium can be defined in terms of difficulty. At a certain difficulty, the income will be low enough and the electricity/hardware costs high enough for an equilibrium to be reached. We predict that when this equilibrium is reached, the difficulty will display an oscillation behavior, not a static behavior due to a cycle.

Fig. 15. Price of 1 Gh/s in BTC from cex.io. [Bitcoinwisdom 2014]

(1) The mining difficulty will approach the equilibrium point. By this time, the mining network will already be under strain from increasing costs and diminishing returns, so it will show a deccelerating behavior.
(2) The mining difficulty will rise above the equilibrium point as the hashrate continues to increase. Whenever the difficulty is over the equilibrium line, most miners will start losing money while mining. Therefore, the total network hashrate will actually go down during the duration of the high difficulty. Only the miners with large captial will continue mining. This trend will continue for 2 weeks.
(3) Since the hashrate went down during the past 2 weeks, the new difficulty will go down, below the equilibrium line. Now that mining is profitable again, miners will once again start mining and increasing their hashrate. People will be able to buy more hardware from their profits, increasing their hashrates.
(4) The cycle will repeat from step 2.

This cycle is diagrammed in Fig. 16, and the resulting difficulty behavior is described in Fig. 17.

The equilibrium line can change due to many factors. If the bitcoin price increases or decreases, the equilibrium line will rise and fall, respectively. Also, if new, cheaper hardware that requires less operational costs is released, the equilibrium line will rise. Therefore, the equilibrium line can be quite dynamic.

This exposes a possiblity for exploitation. When the difficulty is just under the equilibrium line, everyone will mine. However, when the difficulty is over the equilibrium line, the hashrate will drop dramatically has, theoretically, no miner can profit over the equilibrium line, even with the best hardware. This will cause the next difficulty update to be very low, which means miners will be able to mine very profitably at a low difficulty. This will only cause the next difficulty update to be even higher above the equilibrium line, further dropping the overall hashrate. This results in an amplification of the oscillation.

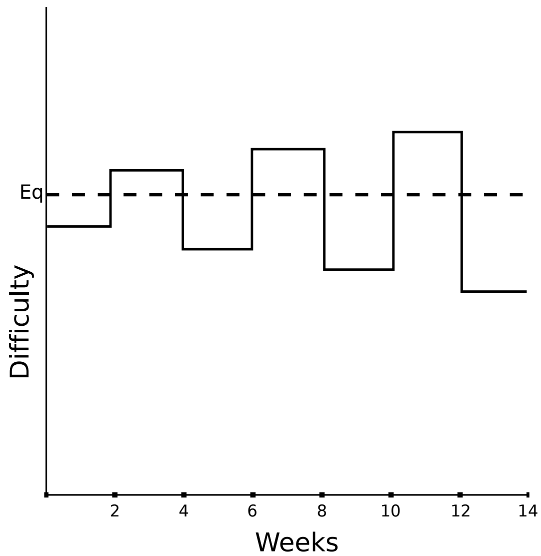


Fig. 16. Difficulty behavior after reaching equilibrium. The dashed line represents the equilibrium.

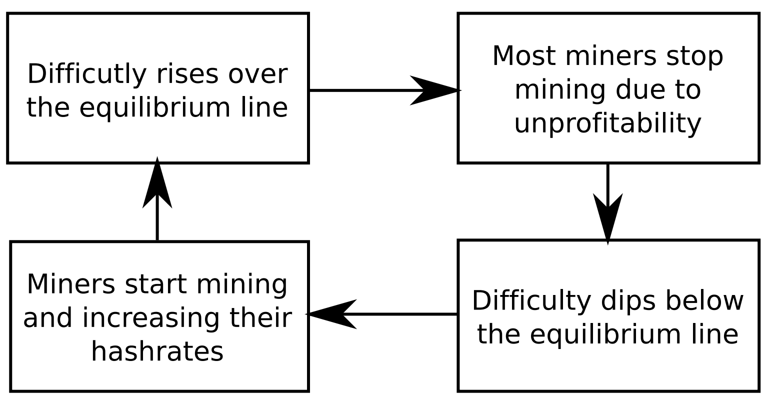


Fig. 17. The mining cycle once the equilibrium is reached.

However, it must be noted that this scenario is extremely unlikely. First, reaching the equilibrium line is extreme, as the difficulty must be high and/or the bitcoin price must be low. For example, at the current electricity usage, bitcoin price, and hashrate, the equilibrium difficulty point is at approximately $2.12 * 10^{11}$ (compared to the actual value of $6.3 * 10^{10}$) under circumstances described in section 4. Or, at the current electricity usage, difficulty, and hashrate, the price of bitcoin would have to be 2.58 USD. Second, we are assuming that all miners are only mining for profit. Even if the equilibrium point is reached under extreme circumstances, it is reasonable to believe that many major miners will continue mining in order to dampen the cycle, as such instabilities may be harmful to the market. Third, this calculation ignores transaction fees; it is possible that transaction fees will keep mining profitable past the equilibrium line.

6. CONCLUSION

In this paper, we analyze various aspects of the mining scene over a period of 15 months in order to understand the overall trend of the bitcoin mining market. We initially find that although the total network hashrate has gone up significantly, the total miner income per month has stayed constant in bitcoin as the network regulates bitcoin generation to 25 btc per 10 minutes. However, due to the volatility of the bitcoin/fiat market, the actual miner income in terms of fiat currency has varied significantly throughout the past.

We discussed the development of mining hardware, and observed the increase of value in bitcoin hardware. It was calculated that despite the increase in hardware value, the hardware costs of the entire mining network increased significantly and accounted for major costs for bitcoin miners. This was tied to a mining strategy of reinvestment and additional investment by external investors.

The energy usage of bitcoin miners was also discussed. We found that despite the increase in efficiency, the increase in hashrate still led to a significant increase in electricity use. Although this electricity use is small compared to the total energy used in the IT sector, electricity use is expected to continue increasing with the development of megawatt datacenters specifically dedicated to bitcoin mining. Electricity costs are not as large as hardware costs, but it is still a main portion of the operation costs, a significant factor in mining profitability.

All of these factors were then combined, and it was found that net miner profits under ideal conditions had crossed into negative net profit in April 2014 under ideal conditions, suggesting that in reality, net miner profit had dipped under zero earlier in the year. This suggests that miners will not be able to continue investment into hardware without large external capital, resulting in a slower hashrate growth in the future.

After discussing past trends, some possible future behavior was discussed in terms of hardware development, hashrate centralization, and mining equilibrium. It was suggested that hardware efficiency development may follow the trend suggested by Koomey's law as bitcoin ASIC technology reaches the current limits of IC technology. It was also suggested that industrial mining centralization may lead to increased chances of a 51% attack, but inherent countermeasures preventing this attack were also discussed. Finally, the possibility of a mining equilibrium was mentioned with the accompanying amplifying oscillation behavior of hashrate and difficulty.

Several assumptions made during calculations and analysis may result in some inaccuracies. All calculations were done assuming that miners will always use the hardware with the best value and best efficiency. It was also assumed that miners immediately converted their bitcoin into fiat currency, which may not be the case. Some miners may be willing to maintain their bitcoins, hoping for a price increase. Bitcoin prices and transaction fees are impossible to predict, and no attempts were made to do so. However, even with these assumptions, the overall trends still give us a very good idea of the behaviors of the mining scene and provide a solid basis to base predictions upon.

REFERENCES

International Energy Agency. 2012. *Electricity Information 2012*. Technical Report. International Energy Agency.

Antminer. 2013. AntMiner S1. Bitmaintech. (November 11 2013). [online; https://bitmaintech.com/productDetail.htm?pid=00020140107162747992Ce5uBuxW06D6].

Antminer. 2014a. AntMiner S2 1TH/s Miner (1w/GH/s) Batch 1 - Sold Out. Bitmaintech. (April 2014). [online; https://www.bitmaintech.com/productDetail.htm?pid=00020140314135446510cxXNeYAy06E5].

Antminer. 2014b. ANTMINER S3 -B3. Bitmaintech. (June 2014). [online; https://bitmaintech.com/productDetail.htm?pid=0002014070402350548 5N5SxDMkW0693].

Avalon. 2014a. Avalon2 Single Module 105. ehash. (January 2014). [online; https://ehash.com/product/avalon2-single-module/].

Avalon. 2014b. Avalon3 machine - 800. ehash. (April 2014). [online; https://ehash.com/product/avalon3-machine-800ghs/].

Avalon. 2014c. Avalon3 Single Module 290. ehash. (April 2014). [online; https://ehash.com/product/avalon3-single-module-300ghs/].

BFL. 2013. Products. Butterfly Labs. (April 10 2013). [online; http://web.archive.org/web/20130410172114/https://products.butterflylabs.com/].

Bitcoin.org. 2014. Bitcoin developer guide. Bitcoin.org. (June 2014). [online; https://bitcoin.org/en/developer-guide].

Bitcoinwisdom. 2014. cex.io market. bitcoinwisdom.com. (October 25 2014). [online; https://bitcoinwisdom.com/markets/cexio/ghsbtc].

BITMAIN. 2013. Announcement: Bitmain launches AntMiner solution, 0.68 J/GH on chip. bitcointalk. (November 11 2013). [online; https://bitcointalk.org/index.php?topic=330665.0].

BitSyncom. 2012. [Announcement] Avalon ASIC Development Status [Batch 1]. bitcointa.lk. (October 24 2012). [online; https://bitcointa.lk/threads/announcement-avalon-asic-development-status-batch-1.71155/].

BlackArrow. 2014a. Bitcoin Miners progress update. Blackarrowsoftware. (July 2014). [online; http://www.blackarrowsoftware.com/store/index.php?dispatch=news.list].

BlackArrow. 2014b. Prospero X-1 (100Ghash/second). Blackarrowsoftware. (July 2014). [online; http://www.blackarrowsoftware.com/store/prospero-x-1.html].

Blockchain. 2014a. Difficulty. Blockchain.info. (July 22 2014). [online; https://blockchain.info/charts/difficulty].

Blockchain. 2014b. Hash Rate. Blockchain.info. (July 22 2014). [online; https://blockchain.info/charts/hash-rate].

Blockchain. 2014c. Hashrate Distribution. Blockchain.info. (October 25 2014). [online; https://blockchain.info/pools?timespan=24hrs].

Blockchain. 2014d. Miners Revenue. Blockchain.info. (July 22 2014). [online; https://blockchain.info/charts/miners-revenue].

Blockchain. 2014e. Total Transaction Fees. Blockchain.info. (July 22 2014). [online; https://blockchain.info/charts/transaction-fees].

Danny Bradbury. 2014. Bitcoin Transaction Fees To Be Slashed Tenfold. CoinDesk. (February 28 2014). [online; http://www.coindesk.com/bitcoin-transaction-fees-slashed-tenfold/].

CoinGazette. 2014. Bitcoin Difficulty Set to Rise Only 3% This Round. CoinGazette. (July 12 2014). [online; http://thecoingazette.com/articles/2014/07/12/bitcoin-difficulty-set-rise-only-3-round].

Christian Decker and Roger Wattenhofer. 2013. Information propagation in the bitcoin network. In *Peer-to-Peer Computing (P2P), 2013 IEEE Thirteenth International Conference on*. IEEE, 1–10.

Stephan Drner. 2014. German Startup Says Its New Chip Halves Bitcoin Mining Energy. Wall Street Journal Digits. (August 15 2014). [online; http://blogs.wsj.com/digits/2014/08/15/german-startup-says-its-new-chip-halves-bitcoin-mining-energy/].

ECDMS. 2014. Electricity Consumption by County. CA.gov. (August 2014). [online; http://www.ecdms.energy.ca.gov/elecbycounty.aspx].

Sydney Ember. 2014. Dell Begins Accepting Bitcoin. New York Times Dealbook. (July 18 2014). [online; http://dealbook.nytimes.com/2014/07/18/dell-begins-accepting-bitcoin/?_php=true&_type=blogs&_r=0].

Katie Fehrenbacher. 2012. The era of the 100 MW data center. Gigaom. (January 31 2012). [online; http://gigaom.com/2012/01/31/the-era-of-the-100-mw-data-center/].

Friedcat. 2013. [Announcement] Block Erupter USB. bitcointalk. (May 4 2013). [online; https://bitcointalk.org/index.php?topic=195004.0].

Google. 2011. What is Googles energy use per user? Google Green. (September 2011). [online; http://www.google.com/green/the-big-picture/references.html].

Nermin Hajdarbegovic. 2014a. Bitcoin Commodity Exchange CEX.io Imposes Trading Fee, Prepares for USD. CoinDesk. (April 2 2014). [online; http://www.coindesk.com/bitcoin-commodity-exchange-cex-io-imposes-trading-fee-prepares-add-usd/].

Nermin Hajdarbegovic. 2014b. BitFury Announces Hosted Mining Services for Business Customers. CoinDesk. (July 31 2014). [online; http://www.coindesk.com/bitfury-announces-hosted-mining-services-business-customers/].

Nermin Hajdarbegovic. 2014c. KnCMiner Finalizes Design For Worlds First 20nm Bitcoin ASIC Miner. CoinDesk. (March 5 2014). [online; http://www.coindesk.com/kncminer-finalizes-design-worlds-first-20nm-bitcoin-asic-miner/].

Alex Hern. 2014. Bitcoin currency could have been destroyed by '51%' attack. The Guardian. (June 16 2014). [online; http://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io].

Kerem Kaskaloglu. 2014. Near Zero Bitcoin Transaction Fees Cannot Last Forever. In *The International Conference on Digital Security and Forensics (DigitalSec2014)*. The Society of Digital Information and Wireless Communications, 91–99.

KnCMiner. 2013. Store Update. KnCMiner News. (September 2 2013). [online; https://www.kncminer.com/news?page=9].

Jonathan G Koomey, Stephen Berard, Marla Sanchez, and Henry Wong. 2011. Implications of historical trends in the electrical efficiency of computing. *Annals of the History of Computing, IEEE* 33, 3 (2011), 46–54.

Bart Lannoo, Sofie Lambert, Ward Van Heddeghem, Mario Pickavet, Fernando Kuipers, George Koutitas, Harris Niavis, Anna Satsiou, Michael Till, Andreas Fischer Beck, and others. 2013. D8.1. Overview of ICT energy consumption. *The EINS Consortium* (February 5 2013).

Daniel Larimer. 2013. *Transactions as Proof-of-Stake*. Technical Report. Invictus Innovations. [online; http://the-iland.net/static/downloads/TransactionsAsProofOfStake.pdf].

Rich Miller. 2014a. Bitcoin Miners Building 10 Megawatt Data Center in Sweden. Data Center Knowledge. (February 6 2014). [online; http://www.datacenterknowledge.com/archives/2014/02/06/bitcoin-miners-building-10-megawatt-data-center-sweden/].

Rich Miller. 2014b. High Density, Low Budget: Massive Bitcoin Mines Spring Up in Warehouses. Data Center Knowledge. (July 10 2014). [online; http://www.datacenterknowledge.com/archives/2014/07/10/massive-bitcoin-mines-spring-up-in-warehouses/].

Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Consulted* 1, 2012 (2008), 28.

Morgen E Peck. 2013. The Bitcoin Arms Race is on! *Spectrum, IEEE* 50, 6 (2013).

Reuters. 2013. Bitcoin miners find it increasingly hard to make money. South China Morning Post. (November 10 2013). [online; http://www.scmp.com/lifestyle/technology/article/1351752/bitcoin-miners-find-it-increasingly-hard-make-money].

Pete Rizzo. 2014a. Bitcoin Mining Giant BitFury Announces $ 20 Million Funding Round. CoinDesk. (May 30 2014). [online; http://www.coindesk.com/bitcoin-mining-giant-bitfury-announces-20-million-funding-round/].

Pete Rizzo. 2014b. Will Industrial Mining Become the Next Big Bitcoin Investment Sector? CoinDesk. (June 15 2014). [online; http://www.coindesk.com/will-industrial-mining-become-next-big-bitcoin-investment-sector/].

Steve Shanafelt. 2014. Mining pool giant GHash.io reaches 50bitcoinx. (June 13 2014). [online; http://www.bitcoinx.com/mining-pool-giant-ghash-io-reaches-50-of-bitcoin-hashing-power/].

Emily Spaven. 2013. KnCMiner begins shipping of Jupiter bitcoin mining rigs. CoinDesk. (October 1 2013). [online; http://www.coindesk.com/kncminer-begins-shipping-jupiter-bitcoin-mining-rigs/].

USEIA. 2013. How much electricity does a typical nuclear power plant generate? eia.org. (December 2013). [online; http://www.eia.gov/tools/faqs/faq.cfm?id=104&t=3].

USEIA. 2014a. Average Retail Price of Electricity, Annual. U.S. Energy Information Administration. (2014). [online; http://www.eia.gov/electricity/data/browser/#/topic/7].

USEIA. 2014b. How much electricity does an American home use? eia.org. (January 2014). [online; http://www.eia.gov/tools/faqs/faq.cfm?id=97&t=3].

Rob Wile. 2013. Bitcoin Developer Sells $8 Million Worth Of Hardware In 24 Hours, As Mining Technology Arms Race Goes Insane. Business Insider. (December 2 2013). [online; http://www.businessinsider.com/knc-sells-8-million-in-miners-2013-11].

Alex Wilhelm. 2014. Popular Bitcoin Mining Pool Promises To Restrict Its Compute Power To Prevent Feared 51% Fiasco. TechCrunch. (July 16 2014). [online; http://techcrunch.com/2014/07/16/popular-bitcoin-mining-pool-promises-to-restrict-its-compute-power-to-prevent-feared-51-fiasco/].

Tim Worstall. 2013. Fascinating Number: Bitcoin Mining Uses $ 15 Million's Worth Of Electricity Every Day. Forbes. (December 3 2013). [online; http://www.forbes.com/sites/timworstall/2013/12/03/fascinating-number-bitcoin-mining-uses-15-millions-worth-of-electricity-every-day].