https://doi.org/10.48009/1_iis_2018_139-149
Issues in Information Systems
Volume 19, Issue 1, pp. 139-149, 2018

CHARGE ME: A COMPARISON OF ELECTRICAL EFFICIENCYIN CRYPTOCURRENCY MINING ALGORITHMS

Isaac R. Cason, Washburn University, isaac.cason@washburn.edu
Aaron Morris, Washburn University, aaron.morris@washburn.edu
Brandon Habig, Washburn University, brandon.habig@washburn.edu
Wenying Sun, Washburn University, nan.sun@washburn.edu

ABSTRACT

Cryptocurrencies rely on computationally expensive cryptographic hashing algorithms to verify transactions. Because mining is necessary for a cryptocurrency to function as a reliable monetary exchange, the power costs must be kept to a minimum to be sustainable. We conducted experiments to look into algorithmic solutions to sustainable cryptocurrencies. During the process, three identical machines were set up and instructed to run mining algorithms for one of three different cryptocurrencies: Ethereum, Monero, and ZCash. Power consumption for each was monitored and logged at intervals of 15 minutes, and then analyzed and tested for differences and statistical significance. Results suggest that the CryptoNight v7 mining algorithm draws a statistically significant lower amount of electrical energy, compared to Ethash and Equihash. We conclude that the choice of mining algorithm should be considered when determining which cryptocurrencies one wishes to mine.

Keywords: Cryptocurrency, Energy Efficiency, Mining, Algorithm, Ethash, Equihash, CryptoNight

INTRODUCTION

Cryptocurrencies are the latest trend to sweep the technosphere. The topic is grabbing the attention of individuals and industries worldwide for good reason. But what exactly is cryptocurrency, and why is it sparking the interests of so many people? Cryptocurrency is a type of currency that is completely digital and is not backed by any government or third party. The USD value of each currency varies from minute to minute. The market value of Bitcoin, one of the most popular and well-known cryptocurrencies, has fluctuated anywhere from around $3,700 per coin in September 2017 to almost $19,000 per coin in December 2017 (CoinMarketCap, 2018). Large fluctuations in market value tend to attract a great amount of attention, lending to the hype surrounding the currency.

One key requirement shared by all cryptocurrencies, however, is that none can function properly, if at all, without a substantial percentage of the network participating in the process of mining. Mining, within the context of cryptocurrencies, is the process of running certain algorithms to hash and verify new transactions added to the blockchain. For each specific currency, the blockchain is a giant public ledger of every transaction to occur. The blockchain is, in essence, a doubly linked list that is extremely secure, with inherent resistance to malicious modification of data. The blockchain also makes use of private and public keys to access one's unique wallet address, enabling secure transactions within the network.

As more and more people start mining, the difficulty goes up and these proof of work algorithms have to work harder to get a high hash rate. Each time a new transaction is successfully mined on a network, the miners are rewarded with newly minted currency, and these rewards tend to be substantial. Given the mining process is very computationally intensive, and as a result draws a significant amount of electrical energy, anyone looking to make a profit from mining cryptocurrencies must work to maximize their hash rate while minimizing power draw. Miners also tend to mine in pools, which allows individual miners to work together and share in the reward when a block is successfully mined. But, as the reward is divided among all miners according to how much work their equipment put in, the resulting reward for each miner is very small, which makes efficiency a necessity.

Although Bitcoin led the charge as one of the earliest and most well-established, many do not realize how large the number of cryptocurrencies available actually is, each with its own different requirements and markets. Three popular cryptocurrencies are Ethereum, which uses the Ethash algorithm, ZCash, which uses the Equihash algorithm, and

Monero, which uses the newest out of the three algorithms, CryptoNight. These three algorithms all use proof of work, but is there a difference in electrical efficiency between the mining algorithms used in each? That is the question we would like to answer. The aim of this research is to conduct a series of experiments and determine whether there is a difference in energy consumption among different cyrptocurrency mining algorithms.

The rest of the paper is organized as follows. We first review existing literature to identify what researchers have done on this topic and if there is any insight that may help our experiments. We then describe the methodology we used to set up and conduct the experiments. Next, we discuss our findings and the impact the findings may have. Lastly, we present the limitations of the study and point out future research that would need to be done to better elucidate the topic.

LITERATURE REVIEW

Few studies have been done on the energy efficiency of mining algorithms. A recent study done at the University of Ireland focuses entirely on Bitcoin, which uses the SHA256 proof-of-work mining algorithm, measuring its energy efficiency. This same study has found that the profitability of a certain type of cryptocurrency is based on a few different factors, including the market value, difficulty, types of hardware being used to mine, and the energy cost of mining (UFD Tech). This study also tested the hash rate, power use, energy efficiency, and cost of a few different CPU, GPU, and ASIC miners. They found that mining with a Central Processing Unit (CPU) yields the lowest hash rate while requiring the highest power consumption, making it the least efficient hardware category. Graphics Processing Units (GPUs) are ranked as a medium between the CPU and Application Specific Integrated Circuit (ASICs) miners with an in-between hash rate and middling total cost to mine. ASIC ranks in at the top of the list as the most efficient to use because of its significantly higher hash rate and significantly lower power consumption, especially when compared to CPUs and GPUs.

The market values of CPUs, GPUs, and ASICs vary ranging from about $50-$250 for a typical CPU (Intel), $300-$1,800 for a typical GPU (Cosmic Shovel, Inc), the price of which has risen dramatically over the past several years as cryptocurrency mining has become increasingly prevalent, and ASICs, which range from about $200-$12,000 (Bitmain). If the value of a Bitcoin is less than the cost of the energy required to generate it then there is not an incentive to continue participating in the mining process. As the number of people mining Bitcoin increases, the difficulty of the mining increases and the likelihood of discovering a valid block decreases.

The algorithms tested in this experiment are very different in their approach. The Equihash algorithm "is a PoW based on the generalized birthday problem and enhanced Wagner's algorithm for it." (Biryukov & Khovratovich, 2016) while Ethash "is a derivative of the Hashimoto algorithm [Dry14] and the Dagger algorithm" (Rudlang, 2017). The CryptoNight algorithm is modeled after networking message security algorithms involving the elliptic curve problem, and public and private keys, etc. (Saberhagen, 2013) A detailed description of each of these algorithms is beyond the scope of this experiment.

METHODOLOGY

In order to test the energy efficiency of the three separate algorithms, three identical computers were used, each mining with a different algorithm. The total and marginal power were measured, where marginal power = total power - baseline power. To get the baseline power, measurements were taken of the computers' power consumption while idle.

Computer setup

Three identical computers were used, each with an AMD RX 570 graphics card as the device that performs the labor intensive part of the cryptocurrency mining. Each computer has an AMD A8 Quad-Core CPU with 4GB of RAM. The hard disk drive is 360GB with Ubuntu Linux as the operating system. This operating system was chosen because of its compatibility with the GPU driver software, and because it has predictable background processes that will not skew the data. The power supply used in each has a rated consumption of 450 watts.

Measuring power consumption

Power consumption is a calculated value, using the power formula,

$$P = IE$$

with P as power (in watts), I as current (intensity in amps), and E as electromotive force (in volts), and then multiplying that value by the duration of time the power level is maintained (EETech Media, LLC). The standard unit for power consumption is kilowatt-hours.

Because of fluctuations in the voltage and current, it is important to take samples with short intervals as quickly as possible. To accomplish this, an Arduino Mega 2560 microcontroller was used to perform the measurements and calculations, and then log the gathered data into a spreadsheet. Using a transformer module to convert the incoming AC power, 120 volt nominal, a sine wave signal is sent to the microcontroller to measure the voltage by calculating the root mean square value. Then, on a custom made circuit board, three inductive coils were mounted, through which the wires supplying three standard receptacles are run. Through the magnetic coupling that occurs with that configuration, a sine wave representing the current running through the wires is sent to the microcontroller, which is then interpreted in a similar method as the voltage (see Figure 1).

The Arduino microcontroller is programmed to sample the current and voltage going to the computers constantly, and then every 15 minutes it writes the collected data to a comma separated values (CSV) file stored on an SD card. Data is collected for approximately one week. This data is then converted to an Excel spreadsheet for statistical analysis.

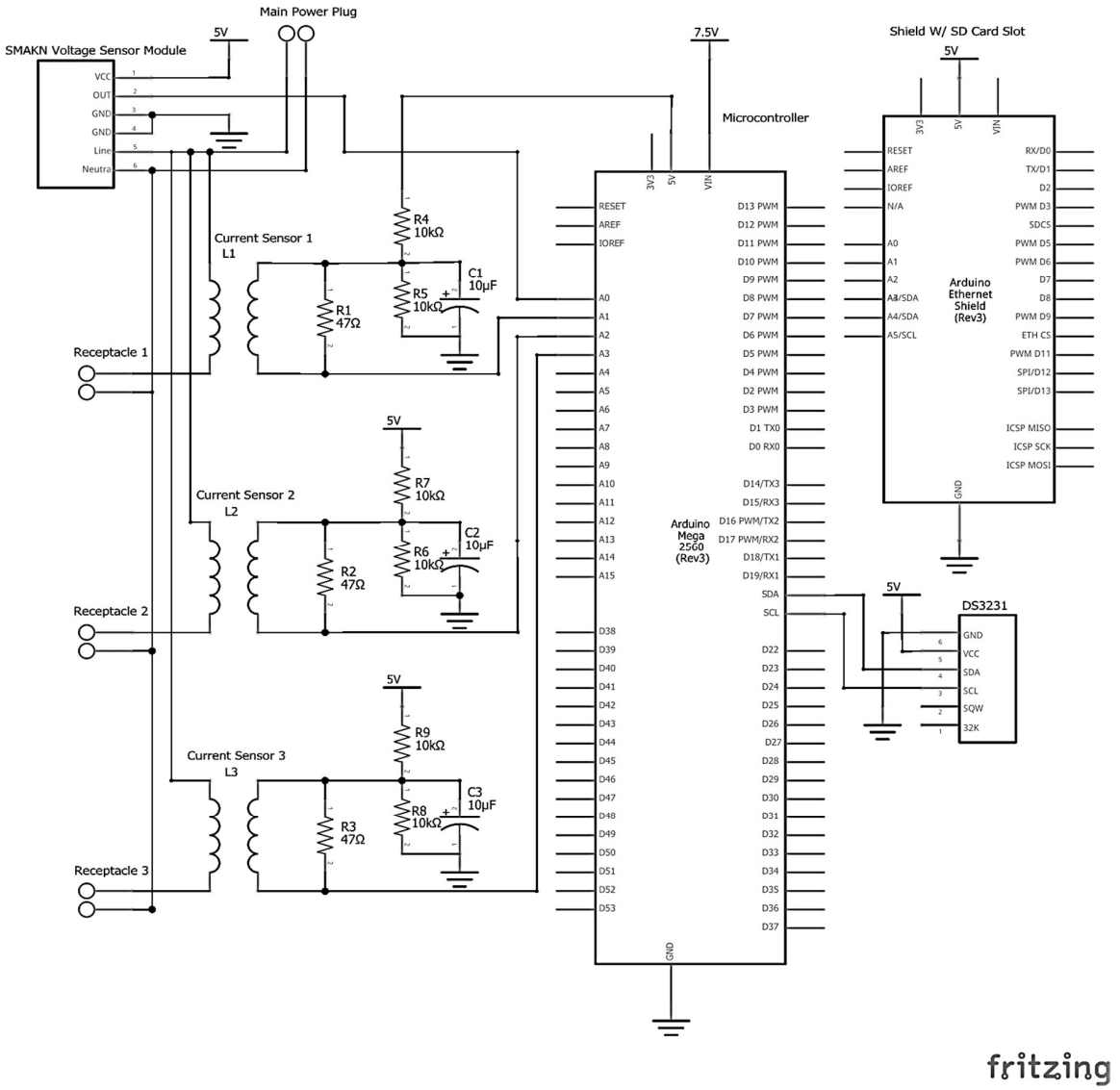

Figure 1. Schematic of Power Measurement Device

Mining software and pools

All three cryptocurrencies could be mined and monitored through miningpoolhub.com.The site required respective accounts to be created for each currency. Also, for each currency, the site provides two or three recommendations for mining software. The Claymore GPU Miner software was installed on each machine. Although Claymore is proprietary software, it functioned more reliably over all three algorithms than the open source options available.

Rounds

Even though the three computers set up were identical in model numbers, it is still desirable to eliminate any variation that may arise due to minor differences in how the units were manufactured. To control for this, the coins were mined in three rounds, switching which currency was mined on each machine (See Table 1).

Table 1. Rounds

	Round 1	Round 2	Round 3
Machine at Input 1	Zcash	Ethereum	Monero
Machine at Input 2	Ethereum	Monero	Zcash
Machine at Input 3	Monero	Zcash	Ethereum

Each round had a duration of approximately 48 hours. The resulting data for each round was analyzed for statistical significance, and then the data from all rounds were compiled into a single file for analysis as a whole using SAS statistical analysis software. To further control for variation in computer hardware, a baseline was measured by monitoring the power consumption of the three computers while they were not mining. All three computers were also monitored while mining with the same algorithm, CryptoNight, under the assumption that mining with the same algorithm with identical equipment will yield identical results. The figures gathered by the idle measurement were then averaged, adjusted according to the identical algorithm test, and then subtracted from the measured power consumption of each computer while mining each coin during each round.

RESULTS

Since the sample size is quite large (665 observations for each currency), a normal one-way analysis of variance test could be run without much concern for normality, though the data does present relatively normal. This test was performed for each round, and then for the data from all rounds compiled together. The summary statistics are found in Table 2.

Table 2. Summary Statistics

Analysis Variable : kWh kWh							
Currency	N Obs	Mean	Std Dev	Minimum	Maximum	Median	N
ETH	665	0.0564734	0.0013794	0.0533278	0.0589102	0.0569741	665
XMR	665	0.0462866	0.0012306	0.0436202	0.0498041	0.0467402	665
ZEC	665	0.0561979	0.0018128	0.0523678	0.0600702	0.0564778	665

Round 1

The null hypothesis for all of these tests is that there is no difference in the energy consumption while the GPUs mine each currency. The results in round one rejects the null in favor of the alternative, namely that the algorithm used does affect energy consumption, and thereby affects profitability. With an R-square of 0.94 the model explains 94.1% of the variance by currency, and has a p-value less than 0.0001 (Table 3). It is interesting to note here that, in the pairwise comparison of the currencies, Ethereum and ZCash are not significantly different while Monero is significantly different from each of the other two (Table 4). The data is visually represented in the line chart in Figure 3, and clearly shows the overlapping of Ehereum and Zcash, while Monero is charted well below the others.

Table 3. Round 1 ANOVA

Dependent Variable: kWh kWh

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	2	0.01860840	0.00930420	4623.93	<.0001
Error	579	0.00116506	0.00000201		
Corrected Total	581	0.01977345			

R-Square	Coeff Var	Root MSE	kWh Mean
0.941080	2.689952	0.001419	0.052734

Table 4. Round 1 Pairwise Comparison

Least Squares Means for effect Currency
Pr > |t| for H0: LSMean(i)=LSMean(j)

Dependent Variable: kWh

i/j	1	2	3
1		<.0001	1.0000
2	<.0001		<.0001
3	1.0000	<.0001	

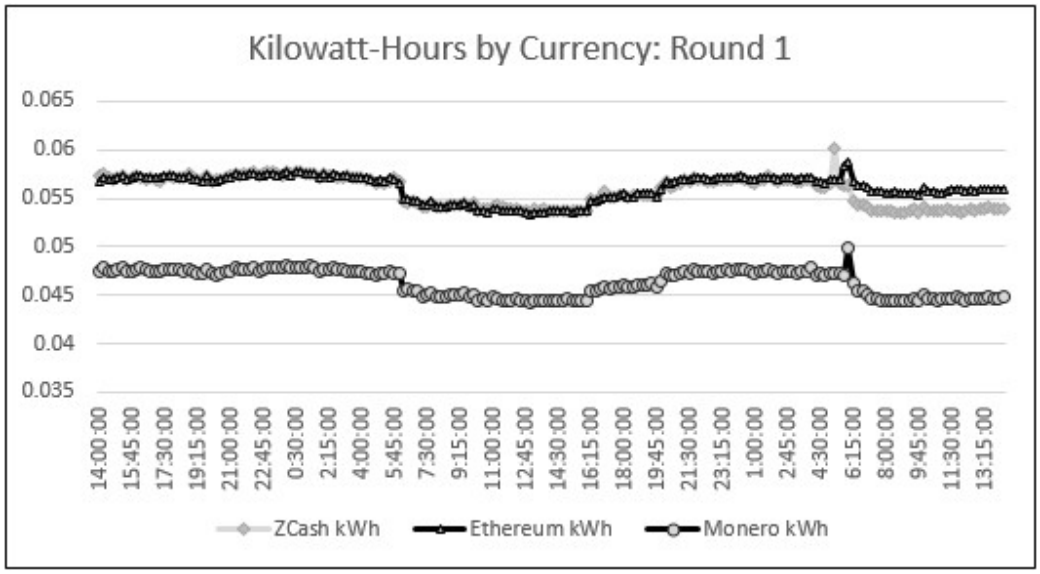

Figure 3. Kilowatt-Hours by Currency: Round 1

Round 2

Again, the null hypothesis is that there is no difference in energy consumption between the currencies being mined. In this round the null hypothesis was again rejected with a p-value less than 0.0001, and an R-square showing the model explains 92.7% of the variance (Table 5). The results from this round do differ from those of Round 1 in that each currency is shown to be statistically different from each other in the pairwise comparisons (Table 6). Charting the data again shows visually how significant these differences are (Figure 4).

Table 5. Round 2 ANOVA

Dependent Variable: kWh kWh

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	2	0.01375188	0.00687594	3550.31	<.0001
Error	558	0.00108069	0.00000194		
Corrected Total	560	0.01483257			

R-Square	Coeff Var	Root MSE	kWh Mean
0.927141	2.629630	0.001392	0.052922

Table 6. Round 2 Pairwise Comparison

Least Squares Means for effect Currency
Pr > |t| for H0: LSMean(i)=LSMean(j)

Dependent Variable: kWh

i/j	1	2	3
1		<.0001	0.0017
2	<.0001		<.0001
3	0.0017	<.0001	

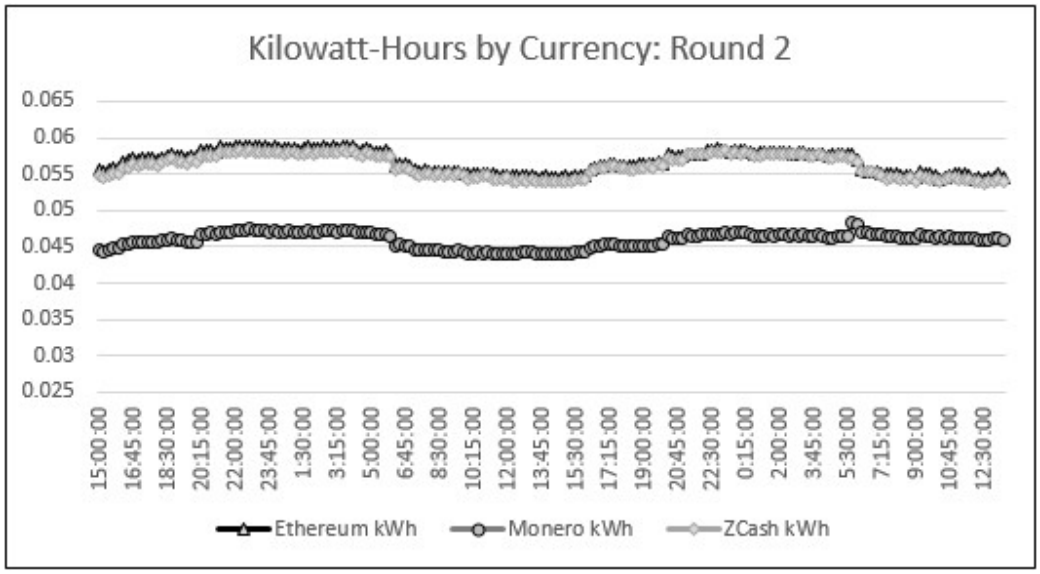

Figure 4. Kilowatt-Hours by Currency: Round 2

Round 3

This round was analyzed the same as the previous two, and had results nearly identical to Round 1. A minor difference is the R-square of 90.3% (Table 7), but again it finds significant difference between the energy consumption of the three algorithms, with the CryptoNight algorithm being more efficient than the other two (Table 8). To visualize the data, once again as a line chart, see Figure 5.

Table 7. Round 3 ANOVA

Dependent Variable: kWh kWh

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	2	0.01920363	0.00960181	3950.80	<.0001
Error	849	0.00206336	0.00000243		
Corrected Total	851	0.02126699			

R-Square	Coeff Var	Root MSE	kWh Mean
0.902978	2.930359	0.001559	0.053200

Table 8. Round 3 Pairwise Comparison

Least Squares Means for effect Currency
Pr > |t| for H0: LSMean(i)=LSMean(j)

Dependent Variable: kWh

i/j	1	2	3
1		<.0001	1.0000
2	<.0001		<.0001
3	1.0000	<.0001	

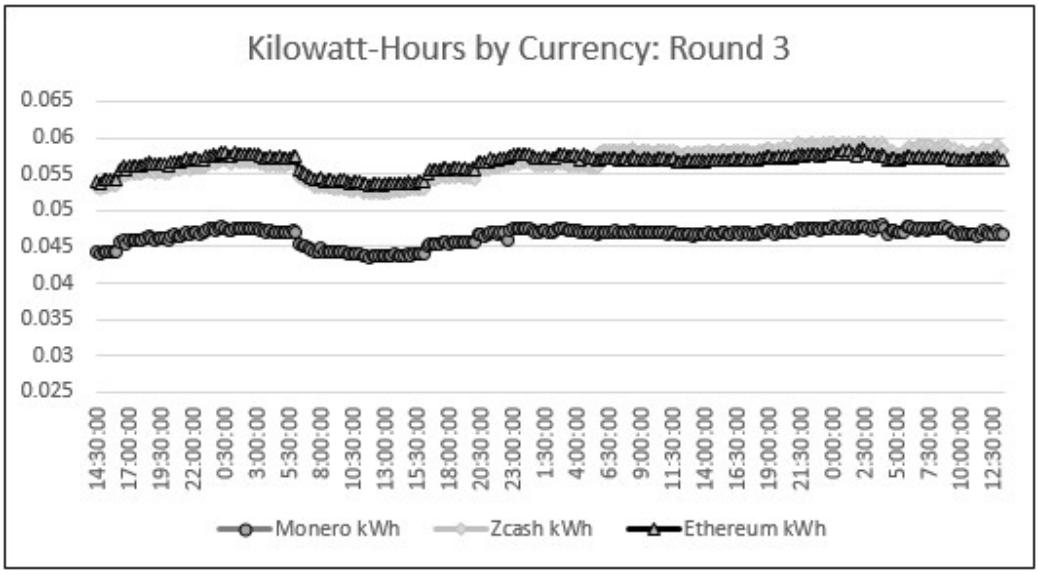

Figure 5. Kilowatt-Hours by Currency: Round 3

All Rounds

Finally, after the data from all three rounds was compiled into one set, it was analyzed as a whole, testing the same null hypothesis as before, and the alternative being that at least one of the currency mining algorithms is different than the rest. The results show very strongly that there is a statistical difference in each of the algorithms. The R-square holds true to the individual round results explaining 90.96% of the variance in energy consumption with choice of algorithm, and a p-value of less than 0.0001 (Table 9). The p-values in the pairwise comparison table are all substantially less than the 0.05 alpha which strongly indicates that each algorithm is significantly different than the other two that were tested in terms of their energy consumption (Table 10). The line plots of all three rounds were stitched together and show the consistency of the results, the differences between the algorithms, and incidentally the daily fluctuations due to power from the grid (See Figure 6).

Table 9. All Rounds ANOVA

Dependent Variable: kWh kWh

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	2	0.04479450	0.02239725	10023.2	<.0001
Error	1992	0.00445119	0.00000223		
Corrected Total	1994	0.04924569			

R-Square	Coeff Var	Root MSE	kWh Mean
0.909613	2.821191	0.001495	0.052986

Table 10. All Rounds Pairwise Comparison

Least Squares Means for effect Currency
Pr > |t| for H0: LSMean(i)=LSMean(j)

Dependent Variable: kWh

i/j	1	2	3
1		<.0001	0.0023
2	<.0001		<.0001
3	0.0023	<.0001	

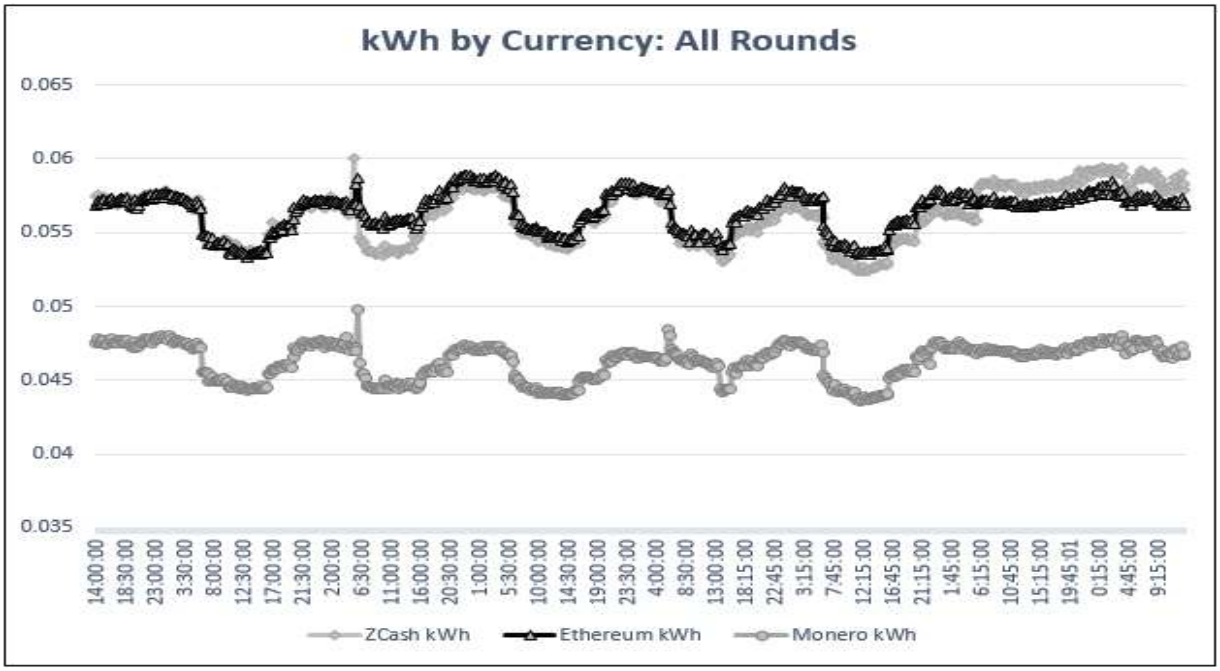

Figure 6. Kilowatt-Hours by Currency: All Rounds

DISCUSSION

GPU mining is an optimal starting position when one is looking to analyze the electrical efficiency of various cryptocurrency mining algorithms: it is a medium in-between CPU and ASIC mining and is a realistic approach a solo miner might take when first joining the mining community. After the Arduino was built and running, the data was gathered and a statistical analysis was performed on the data. After multiple rounds and tests were conducted, the conclusion was that the Ethash algorithm was the least efficient with a mean 15-minute consumption rate of 0.0565

kilowatt-hours, the Equihash algorithm was slightly more efficient at 0.0562 kilowatt-hours, leaving the CryptoNight algorithm as the most efficient with a mean 15-minute consumption rate of 0.0463 kilowatt-hours (Table 1). This experiment shows, at least among the algorithms tested, that choice of algorithm should be considered when embarking on a crypto mining endeavor.

As this research shows, there is a lot behind the scenes of digital cryptocurrency that, despite its socially trending status, many are not aware of. Even though research has been done on Bitcoin, the results seem to be consistent among different currencies: CPU mining is inefficient and has few uses beyond purely academic purposes, and GPU mining, although still somewhat relevant, is quickly being overtaken by ASIC mining. The key difficulty with ASIC mining pertains to cost: ASICs are very expensive to manufacture, and are usually mined with first to maximize profit before being sold second-hand to the general public. That said, larger companies with capital to spare can invest in large farms of ASICs and quickly come to dominate any particular cryptocurrency, which can provide a significant threat to the distributed nature of a cryptocurrency.

Based on our research CryptoNight v7 is the most efficient cryptocurrency mining algorithm out of the three that were tested. This is an impactful revelation because energy consumption is an extremely important cost to consider when choosing to actively mine cryptocurrencies. Miners have many choices to make in order to maximize their profit: they must choose affordable hardware that can recover its initial cost in a reasonable amount of time, they must choose a coin to mine that has sufficient market value to be profitable, is sufficiently easy to exchange or spend, and that has a difficulty level appropriate to the chosen equipment. An interesting correlation is that the lower the market-value of the coin, the higher the efficiency of the algorithm appeared to be. This study shows that miners could use a choice of algorithms to narrow down what coins to mine that will minimize the electricity expense. If one is looking to mine for profit among the three currencies tested here, it is best to go with a coin that uses the CryptoNight v7 algorithm.

CONCLUSION, LIMITATIONS, AND FUTURE RESEARCH

In this research, we set up three identical machines to run mining algorithms for three different cryptocurrencies: Ethereum, Monero, and Zcash. The Arduino microcontroller was programmed to sample the power consumption and to write the collected data to a comma separated values (CSV) file every 15 minutes. The coins were mined in three rounds, switching which currency was mined on each machine. Each round had a duration of approximately 48 hours, which yielded about 665 observations for each currency. Statistical analysis was performed for each round, and then for the data from all rounds compiled together. Results suggest that the CryptoNight v7 mining algorithm draws a statistically significant lower amount of electrical energy, compared to Ethash and Equihash, therefore, is the most efficient cryptocurrency mining algorithm out of the three.

A number of things could be done to expand the depth and quality of the presented research. The first limitation is a simple matter of scale. Given that there are more than 800 different cryptocurrencies, according to coinmarketcap.com, it would take a setup of much more than three machines and a meager few weeks to fully explore and research them all in any reasonable amount of time, especially before any data collected becomes too far out of date. The second limitation involves the hardware used during testing. All tests conducted as part of this research were conducted using AMD RX570s, a lower-middle tier graphics card. Expanding the range of graphics cards used would provide increased depth to the data by exposing any potential energy efficiency differences between the cards themselves, which would directly influence energy efficiency of the mining algorithms. Beyond that, Application Specific Integrated Circuits, or ASICs, are in the process of dominating the market, and by their nature are both faster and more energy efficient than a GPU.

ASICs provide an opportunity for future research. Despite the sunk cost in creating or acquiring an ASIC, their reported advantages pose a threat to the distributed nature of every cryptocurrency, and create potential to abuse the network of their target coin. Further research could include, among other things, investigation into the development of an ASIC-proof or, at the very least, further ASIC-resistant mining algorithms. Such a development could level the playing field between those capable of utilizing ASICs and those who cannot, while giving GPU mining systems back their edge, and preserving the decentralization necessary for secure cryptocurrencies.

REFERENCES

Biryukov, A., & Khovratovich, D. (2016, February). *Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem* [Scholarly project]. In *Orbilu.uni.lu*. Retrieved May 04, 2018, from http://orbilu.uni.lu/bitstream/10993/22277/2/946.pdf

Bitmain. (n.d.). Bitmain. Retrieved May 04, 2018, from https://shop.bitmain.com/?lang=en

CoinMarketCap. (2018, May 04). All Coins. Retrieved from https://coinmarketcap.com/coins/views/all/

Cosmic Shovel, Inc. (n.d.). Amazon Price History for GPU. Retrieved May 04, 2018, from https://camelcamelcamel.com/XFX-Radeon-Graphic-Karten-rx-vegmtbfx6/product/B074DK6NHQ

EETech Media, LLC. (n.d.). Power in Electric Circuits. Retrieved May 04, 2018, from https://www.allaboutcircuits.com/textbook/direct-current/chpt-2/power-electric-circuits/

Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem [Scholarly project]. In Orbilu.uni.lu. Retrieved May 04, 2018, from http://orbilu.uni.lu/bitstream/10993/22277/2/946.pdf

Intel. (n.d.). Intel® Core™ Processors. Retrieved May 04, 2018, from https://www.intel.com/content/www/us/en/products/processors/core.html?cid=sem43700027471227926&intel_term=intelcpu&gclid=Cj0KCQjw5qrXBRC3ARIsAJq3bwojhUXHd92XzkdC7-9Y7oqrQv1y2bJO5jolyWWqzXeUAhGMiP4IflUaAuziEALw_wcB&gclsrc=aw.ds&dclid=CPn6gfm069oCFcRvAQodWloIGw

O'Dwyer, K. J., & Malone, D. (2014, June 26). *Bitcoin Mining and its Energy Footprint* [Scholarly project]. In *Eprints.maynoothuniversity.ie*. Retrieved May 04, 2018, from http://eprints.maynoothuniversity.ie/6009/1/DM-Bitcoin.pdf

Rudlang, M. (2017, June). *Comparative Analysis of Bitcoin and Ethereum* [Scholarly project]. In *Https://brage.bibsys.no*. Retrieved May 04, 2018, from Biryukov, A., & Khovratovich, D. (2016, February).

Saberhagen, N. V. (2013, October 17). *CryptoNote v 2.0* [Scholarly project]. In *Https://cryptonote.org*. Retrieved May 04, 2018, from https://cryptonote.org/whitepaper.pdf

UFD Tech. (n.d.). Home[YouTube Channel]. Retrieved from https://www.youtube.com/channel/UC4Z8mPYjn6Dhr6n531YDh0Q