Journal of Theoretical and Applied Information Technology
15th March 2019. Vol.97. No 5

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PROOF OF WORK: ENERGY INEFFICIENCY AND PROFITABILITY

[1]ANAK AGUNG GDE AGUNG, [2]RIXARD G. DILLAK, [3]DEVIE R. SUCHENDRA, [4]ROBBI H.
[1,2,3,4]School of Applied Science, Telkom University, Indonesia
E-mail: [1]agung@tass.telkomuniversity.ac.id, [2]rixard@tass.telkomuniversity.ac.id,
[3]deviersuchendra@tass.telkomuniversity.ac.id, [4]robbi@tass.telkomuniversity.ac.id

ABSTRACT

Decentralized and immutable characteristic of blockchain has a possibility to change how the data is stored. Cryptocurrency is one example of successful blockchain technology implementation. The first cryptocurrency, bitcoin, was launched in 2009 and shortly afterwards followed by other cryptocurrencies, which are called alternative currency (altcoin). The blockchain system depends on a consensus mechanism to run. Most of cryptocurrency adopt the Proof of Work (PoW) consensus mechanism, which requires to run a computer program to solve a computational puzzle to verify the transactions and add the record into the blockchain, which called mining. Bitcoin uses SHA258 algorithm for its PoW. As an incentive, miners are then given some money on the currency. However, mining requires a lot of energy, alternatively, altcoins adopt different algorithm to run the system. This study aims to compare the energy used by various algorithms, which mined by four widely available, general purposes Graphic Processing Unit (GPU), and determine the profitability for each currency, given the mining share acquired for 24 hours. This is important because even the blockchain is not intended primarily for cryptocurrency, PoW-based blockchain system depends heavily on the mining process. Should the miners decided it is no longer profitable, they will easily switch to mine another, and without miners, the blockchain system will stop. The experiment shows that from 32 sets of experiment, only 15 sets (46.88%) are profitable. The result shows that among eight algorithms, Equihash, Ethash, and Cryptonight7 coins are the best performers, while Blake2b, Blake256, and Lyra2REv2 coins are the worst performers. Most the coins tested consume below than 1 TWh of annual energy consumption, except SiaCoin and Ethereum, and Decred.

Keywords: *Cryptocurrency, Altcoin, Proof-Of-Work, Energy, Profitability*

1. INTRODUCTION

The first cryptocurrency, bitcoin (BTC) was launched in January 2009 based on Satoshi Nakamoto's paper [1]. Ever since, other cryptocurrencies have been emerged. Bitcoin (BTC) and altcoins (alternate cryptocurrencies, community name for cryptocurrencies other than BTC) are gaining popularity, reached their peak in the end of 2017. At the time this article was written, there are 792 cryptocurrencies available in the market, with the total market capitalization worth of $232,993,580,527 [2].

One reason for bitcoin and other cryptocurrencies popularity is that they require a much lower transaction fee than credit cards and exchanges, which charge 1% to 3% of the transaction value [3]. Cryptocurrency is also characterized by its anonymous and decentralized processing of transactions. Figure 1 shows the transaction volume of bitcoin (BTC), which reach USD 48.35 billion on December 13, 2017, while Ethereum (ETH) reach USD 20.32 billion and Ripple (XLM), reach USD 6.33171 million on January 4, 2018.

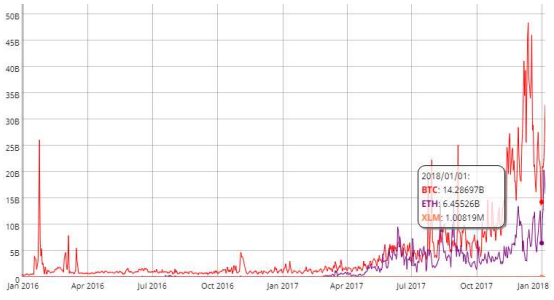

Figure 1: Transaction Volume (USD) for Bitcoin (BTC; red), Ethereum (ETH; purple) and Stellar (XLM; yellow)

Unlike traditional banking system, validation of transaction in cryptocurrency does not rely on single entity. It does not rely on central bank nor government. Instead, transaction is verified using a consensus mechanism involving multiple parties. Every party (which is called a node) runs a specific computer program in accordance of the mechanism

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

adopted by the currency. In cryptocurrency system, a node plays a very important role. They validate transactions and record valid transaction into the blockchain. In general, there are three mechanisms to validate the transaction of cryptocurrency, the Proof of Work (PoW), the Proof of Stake (PoS) and masternode.

The PoW is used by 542 cryptocurrencies, or roughly 68% of all cryptocurrency. In PoW mechanism, a node runs a process called mining. While mining is a mandatory process, it consumes a great amount of electricity [4]. As an incentive, miners are given shares in the form of the cryptocurrency he or she mined. Bitcoin is an example of PoW based cryptocurrency which uses the SHA256 algorithm. Previous research on bitcoin mining revealed a conclusion that in 2004, electricity needed to mine bitcoin alone is comparable to Ireland's electricity consumption [5]. Figure 2 shows electricity consumption for bitcoin mining annually in January 1, 2018 had reached 36.79 TWh, and it keeps rising [6]. This fact raises concern that mining bitcoin will not be sustainable in the near future [7] [8] [9].

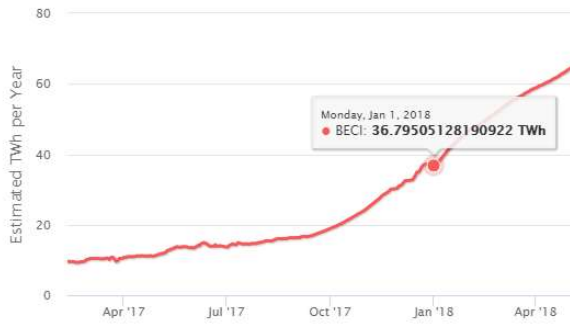

Figure 2: Bitcoin Energy Consumption Index (BECI) Chart

Cryptocurrency developers are trying to use another algorithm rather than bitcoin's SHA256. In addition, to speed up the transaction, other purpose is to reduce power consumption, because the simpler algorithm uses less computing power and less load on the hardware. By the time this manuscript was written, there were more than fifty algorithm used by cyrptocurrencies.

Cryptocurrencies use blockchain technology, but the blockchain application is not limited to cryptocurrency. While many argue that cryptocurrency might not mature enough to replace the current monetary system, the blockchain technology has a potential implementation in many fields. Research and implementation of blockchain includes smart contract, logistics [10] [11], taxation [12] [13], energy industry [14], also health and medical [15] [16] [17] area.

Profitability is a major reason for miners to join the mining process. For PoW based blockchain, loosing miners could cause a problem, as the system relies on miners to run the validate transactions. Less miner also means the system becomes more centralized. It is important to keep the mining process profitable to attract miners.

This research compares energy used by GPU mining. The obtained share then converted to fiat money (USD) to determine if it is still profitable. We also estimate how much energy needed and how much it cost to run the network Eight algorithms, represented by eight altcoins are used in this research. This should provide an overview on how a different consensus algorithm makes an impact to mining profitability in actual condition.

2. DIGITAL MONEY

Money refers to anything, which generally accepted, by a community, as a medium of exchange. Money can have physical object, such as coins or papers, which we know as cash. This type of money has its value written on it. When it is recognized by the legal system in a country, it is known as legal tender. Digital money is the electronic equivalent of cash. It exists in the form of a data file, stored in a hardware or software. It circulates in electronic network and transactions are carried out electronically [18] [19]. Since digital money exists in the form of data, it can be duplicated at negligible cost. This is a problem known as the "double spending problem". To solve with the double spending problem, digital money transaction involves a central authority, which keeps track the ownership of the money and verify the transactions. This central authority is usually a bank or a government agency. However, this centralized system requires trust that the central authority will not abuse the delegated power. Since there is only one central authority, the system also vulnerable to various problems, such as technical failure, hackers attack on the database, or even malicious parties.

3. CRYPTOCURRENCY

Currency is money, which is acknowledged and circulated in a specific boundary (such as country) [20]. Currency can exist in physical and digital form. Currency can be regulated by the government, or unregulated (virtual). Virtual currencies usually created and used by virtual communities. Different from regulated currency, which has geographic boundary, virtual currency has no geographic boundary. In digital, virtual money, anyone

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

connected to the internet can be part of the community, regardless his or her geographic location. Cryptocurrency is a virtual, digital money, which uses cryptography in its transaction and creation. It has no intrinsic value, and their value represents entirely on the expectation of the currency. The first cryptocurrency is Bitcoin, which was launched in January 2009. There are many cryptocurrencies created after bitcoin, known as alternate coin (altcoin) or simply called coin. Cryptocurrency uses blockchain technology to store its transaction data, which eliminate the double spending problem of digital money.

4. BLOCKCHAIN

In distributed ledger system, the transaction records are stored in a ledger, and duplicated and keep by multiple entities or nodes. These nodes communicate and update their ledger when a transaction occurred, so every entity would keep the same, updated ledger. Any disputes regarding a transaction would be settled in a consensus way. This means to successfully attack the system, one must have at least 50% plus one of all entities. The first known use of the system was practiced by the people on the small island in the Pacific Ocean called Yap [21].

Transaction records in the blockchain are stored in a block, and cryptographically linked to the previous block to form a chain (which is called blockchain) as a security measure (Figure 3). The bitcoin blockchain uses SHA-256 hash function to secure its data.

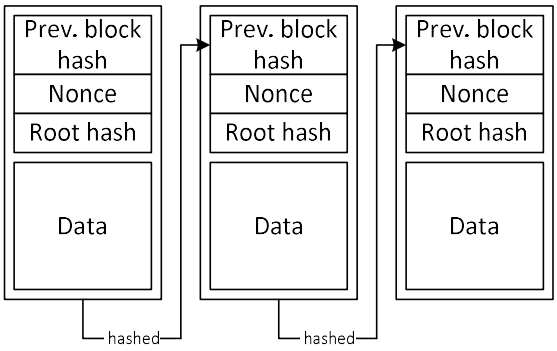

Figure 3: Blocks in a Blockchain

The blockchain then is replicated across the network. Entities which maintain the blockchain is known as a node, a computer which runs a specific program that corresponds to the type of consensus mechanism being used. There are many consensus mechanisms available, but the majority used are the Proof of Work and the Proof of Stake. The use of hash function means we can easily check if a transaction record is changed, and since the hash of a block is linked to the next block, any attempt to change a transaction in specific block must be followed by changing the hash of every block afterward. Even if this is possible, the network will easily detect this false blockchain because other nodes in the network still have the correct blockchain. This makes the blockchain immutable.

Despite its unregulated and their value depend completely to supply and demand, cryptocurrency has advantages, as they inherit the nature of the blockchain. A blockchain is immutable, it is secured by hash chain and every node in the network has its copy. It also spread the authority among the nodes, which means any data added should be decided by consensus, eliminating single point of failure. It is transparent, everyone can see every transaction from the beginning, which also means users can easily trace the transaction history.

Successful implementation of blockchain technology in cryptocurrency opens the possibility for other industry do adopt it. Transaction data could be replaced with any other data, depends on its application. The nature of blockchain can disrupt security industry, financial sector, public services industry, and Internet of Things we already know [4].

4.1. Proof of Work (PoW)

In PoW based cryptocurrency, miners collect and verify pending transactions. Pending transactions are assembled in a block candidate. However, there can be only one block candidate added to the blockchain at a time. To choose which miner can add the block, miners compete to solve a computational puzzle, to hash value below a certain threshold, which is called difficulty. Solving a puzzle prove that a miner has made a contribution to the network, and not likely to perform something malicious. This is a better approach rather than randomly choose a miner [22]. Beside the pending transactions, a miner adds an incentive transaction to its own account, makes every miner start solving the puzzle with different numbers. A random number, nonce, is included in the calculation. In a simple way, mining is to find a nonce which produces a hash lower than the difficulty.

The computational power of a miner is denoted in Hash per Second (H/s). The first miner to complete the puzzle have the right to add the block candidate to the blockchain, and receive an incentive, which is meant to compensate the miner for his or her work. The incentive mechanism is the major reason for people to mine cryptocurrency. So in short, the main

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

purpose of mining is to check transaction validity as well as to create new money [23].

For most cryptocurrency, mining is permissionless. Everyone can download the mining software and the latest blockchain. More miner joins the system will increase the probability to solve the puzzle faster, however, only one block can be added to the blockchain in certain time. To maintain a constant block time, the network adjusts the puzzle difficulty periodically, in which every miner must find a hash number below the difficulty value.

If there is no miner, no one will verify the transaction and the whole system will shut down [24], so in PoW mechanism, the incentive share must be profitable enough to attract miners and cover their expenses.

The mining process itself involves computing power to calculate the cryptographic hash, along with the information of the transaction. The most common way, it utilizes the Central Processing Unit (CPU) or Graphic Processing Unit (GPU) computing power. A miner runs the mining program either on a Personal Computer or in special hardware called Application Specific Integrated Circuits (ASIC). Newer cryptocurrencies such as Electroneum (ETN) is designed so it can be mined using mobile device [25]. The ASIC produces a very high hash rate, but they are very expensive, and the algorithm is limited for every machine. The CPU is the least expensive hardware, but the hash rate is very low compared to the others. This is the reason most miners use GPU for mining process. Here we will put forward brief introduction the consensus algorithms, which are used in the research.

4.1.1 Ethash [26]

The Ethash is the consensus algorithm of Ethereum based blockchain. It is derived from Dagger-Hashimoto algorithm, and designed to be ASIC resistant. The Ethash is similar to bitcoin's algorithm, which is to hash a block candidate header and the result should be below a certain number, or difficulty.

Not only changing the nonce, this algorithm requires miners to add pieces of data from a dataset (DAG). Rather than hashing function, the algorithm focuses on the input / output operation of a computer.

4.1.2 Cryptonight [27]

Cryptonight utilizes memory. In cryptonight, a large area of memory is used to store pseudo-random value. Then, a numerous read/write is performed at pseudo-random addresses contained in the memory. Final operation is to hash the entire memory. The operation also involves Keccak algorithm. Cryptonight7 includes two modifications to the original algorithm.

4.1.3 Equihash [28]

Equihash is designed based on the generalized birthday problem. The algorithm requires some minimum amount of memory to solve the puzzle efficiently, while the verification process is very fast, and the solution is very small. The algorithm was designed to be ASIC resistant.

4.1.4 X17

The X17 is based on X11 algorithm [29]. It consists of 13 hashes cycle, each with different hashing functions (Blake, BMW, CubeHash, Djb2, Echo, Fugue, Groestl, Hamsi, JH, Keccak, Loselose, Luffa, Simd, Shabal, Shavite, Skein, Whirpool). The result of the first hash is calculated with the next algorithm, and so on. The algorithm considered to be safer than Bitcoin's SHA-256. The first coin uses the algorithm was the People (PPL) but the coin is currently discontinued.

4.1.5 Blake2b / Blake256 [30]

Blake2b is a second generation of Blake family cryptographic hash function, which is optimized for 64-bit platform, and the other, Blake2s is optimized for the 32-bit platform. The algorithm focuses on CPU computational power, and utilizes modern processor architecture, such as instruction-level parallelism, SIMD instructions, and multiple cores CPU. The Blake2 algorithm initially created to replace MD5 and SHA-1 algorithm.

Blake256 is the predecessor of Blake2s and derived from the first generation of the Blake family. Instead of 16 calculation rounds in the Blake2b, The Blake256 only has 10. It uses 32-bit words and produces a 256-bit digest.

4.1.6 Scrypt [31]

The Scrypt was originally created as a protection for online backup service. Cryptocurrency adopted the simplify version of the algorithm. The script has memory intensive algorithm, which requires a certain amount of memory to operate. The basic operation is to complicate the solution of cryptographic task with randomly generated numbers.

4.1.7 Lyra2REv2

Lyra2REv2 is an improvement of Lyra2 algorithm, which is a key derivation function. In Lyra2, the memory and processing power can be tuned so users can specify the level of security [32]. The Lyra2REv2 is the second version of reduced

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

efficiency of Lyra2. It consists of a six chained hashes with five hash functions, Blake, Keccak, Cubehash, Lyra2, Skein, Cubehash, BMW. Second round of the Cubehash was added to reduce CPU effectiveness, which was caused by bot mining.

4.2. Mining Pool

Early days mining did not require a lot of computational power. As more people join the process, it is harder to compete. People with higher hash power will have better possibilities to solve the PoW puzzle first, and will have better possibilities to get the incentive. To achieve higher hash, miners work together and combine their computational power in a mining pool. Solo mining was unpractical since it would take days to solve the puzzle. However, by joining the mining pool, the incentive has to be shared among all miners in that pool.

There are more than ten major mining pool, most of them are located in China. Figure 5 shows mining pool in the world. Percentages show total incentive acquired within 48 hours [33].

5. RESEARCH METHOD

The overview of the research steps is presented in Figure 4, which explained below.

First, we select eight altcoins (non-SHA256) which have different algorithms. They should be GPU mineable, and the coins should be listed in top 100 market capitalization, based on data from CoinMarketCap website [34], March 13, 2018.

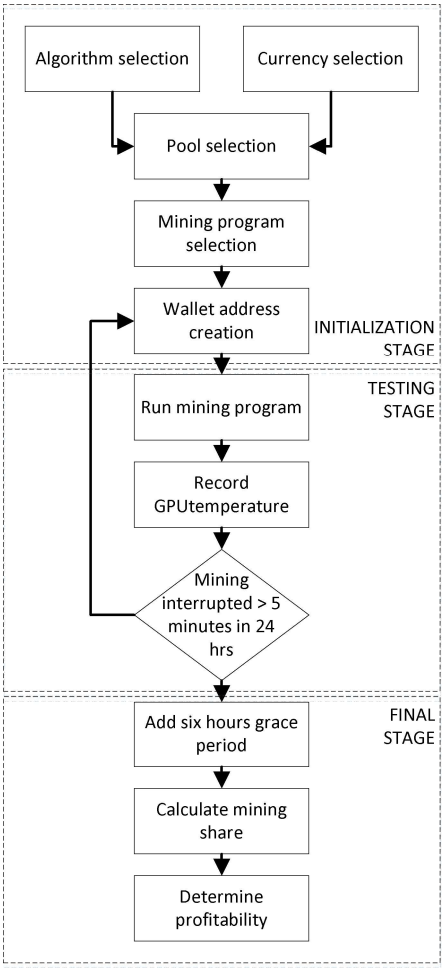

Figure 4: Research Flowchart

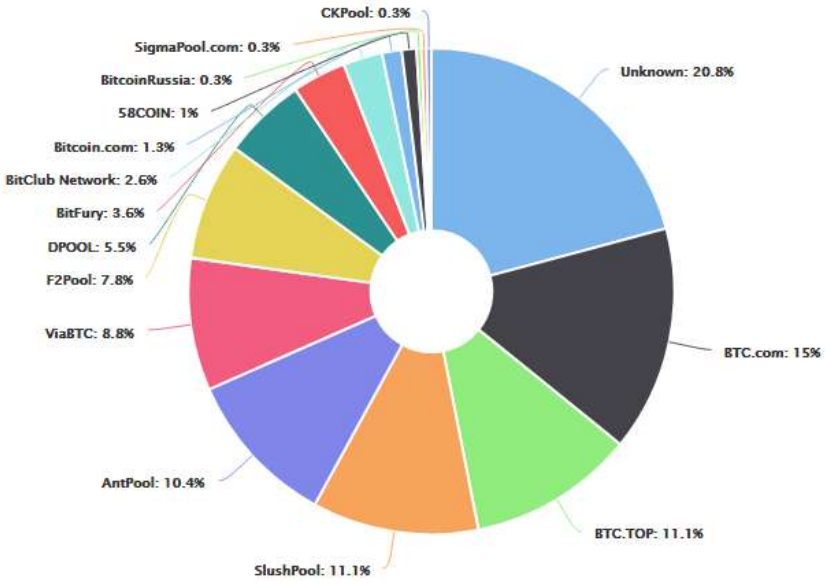

Figure 5: Bitcoin Mining Pool

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

If there are cryptocurrency with the same algorithm, the one with the highest market capitalization is chosen. Higher market capitalization means the coin is established and more stable. Table 1 shows the complete list of the cryptocurrencies in this research.

Table 1: Selected Coin

No	Rank	Coin	Algorithm
1	2	Ethereum (ETH)	Ethash
2	5	Monero (XMR)	Cryptonight7
3	10	Bitcoin Gold (BTG)	Equihash
4	13	Verge (XVG)	X17
5	12	Siacoin (SC)	Blake2b
6	11	Decred (DCR)	Blake256
7	20	MonaCoin (MONA)	Scrypt
8	57	Feather Coin (FTC)	Lyra2REv2

After the cryptocurrencies are selected, mining pool, in which the mining program will connect to, is selected. Table 2 describes mining pool for each coin. The appropriate mining program for each algorithm and GPU is selected, and the wallet address for each currency is generated. The address is used to save incentive of the mining.

The NVIDIA GeForce GTX 1080Ti and ATI Radeon RX Vega 64 represent two high-end consumer (general purpose) GPU available in the market, listed at number one, and number seven on the graphic card benchmark. Both are listed at the top from their respective manufacturer. The nVidia GeForce GTX 1070 and ATI Radeon RX570 represent much affordable GPU, listed at number 13 and 35 on the benchmark list [35]. All four GPUs are listed as high-end graphic cards. The GPU is selected because it is affordable enough for most people, and widely available. They produce a better hash rate than CPUs, and less expensive than ASICs.

Table 2: Mining Pool

No	Coin	Pool
1	Ethereum (ETH)	asia1.ethermine.org
2	Monero (XMR)	aus01.supportxmr.com
3	bitcoin Gold (BTG)	asia.btgpool.pro
4	Verge (XVG)	hashfaster.com
5	SiaCoin (SC)	asia.siamining.com
6	Decred (DCR)	dcr.coinmine.pl
7	MonaCoin (MONA)	miningpoolhub.com
8	FeatherCoin (FTC)	miningpoolhub.com

Table 3 shows mining program details used for each currency. The mining program ran for 24 hours for each currency. Configuration for each mining program was set to default. Tweaking was performed only if default configuration causes error (system freezes, restart or shutdown). If the mining program was interrupted more than five minutes, the mining process was repeated, and new address was generated.

Table 3: Mining Program

Coin	Mining Program	
	nVidia Cards	AMD Cards
Ethereum (ETH)	ETH Claymore Miner v11.7 AMD-NVIDIA Windows	
Monero (XMR)	XMR-Stak 2.4.2 (April 19, 2018)	
bitcoin Gold (BTG)	EBFZec Miner 0.3.4.b	Claymore's Zcash - AMD GPU Miner v.12.6
Verge (XVG)	ccminer/alexis-1.0	sgminer/5.5.5-aeris
Siacoin (SC)	ccminer-800-x64-cuda75	marlin-0.9.0-win32
Decred (DCR)	gominer OpenCL v.1.0.0	
MonaCoin (MONA)	Ccminer x64 2.2.3 CUDA 9	Sgminer 5.6.1. nicehash 51*; Sgminer 5.5.4.3**
Feather Coin (FTC)	CCMiner 2.2.5	Claymore's NeoScrypt AMD GPU Miner v1.2

* RX Vega 64, ** RX 570

Table 4 shows the complete specification of the computer system. All mining programs are set to use only the external GPU, while the on-board GPU exclusively connected to display monitor to ensure uninterrupted mining process.

Table 4: Hardware Specification

No	Component	Specification
1	Motherboard	Asus B250 Mining Expert, Skylake-B250

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

No	Component	Specification
		chipset, Intel HD Graphic 510
2	Memory	16GB (2x8GB) DDR4 1066 MHz dual channel
3	CPU	Intel Skylake G4400 @ 3.30GHz
4	GPU-0	Galax nVidia GeForce GTX 1080Ti 11GB GDDR5X @ 1630MHz
5	GPU-1	MSI nVidia GeForce GTX 1070 8GB DDR5 @ 1582MHz
6	GPU-2	MSI Radeon RX Vega 64 8GB HBM2 @ 1630MHz
7	GPU-3	MSI Radeon RX 570 4GB GDDR5 @ 1281MHz
8	Hard drive	Seagate ST3500418AS 500 GB, SATA 3Gb/s
9	Power Supply	Corsair HX1000 (1000 W) + Enlight ENP-750HP (750 W)

All four external GPUs are connected using PCIe riser, as shown in Figure 6.

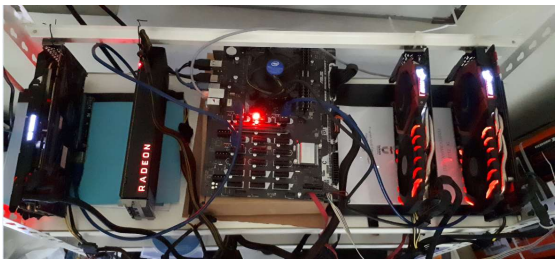

Figure 6: GPU Configuration

The setup run on the latest Windows 10 Pro, set to default configuration except for the Virtual Memory is set to 400 GB and windows update is turned off. All nVidia cards use the official v.388.71 driver, while the AMD cards use the official v.24.20.11001.5003 driver. The computer is placed in a 25°C temperature room.

The mining program runs for 24 hours for every coin. A six-hour grace period is added after the mining program finished to let all share completely confirmed by the network before they are collected at the wallet. Another extra time can be added to let the 'dust' being collected. In some mining pool, balance below a certain value (dust) can only be transferred into the wallet in a specific period, for example every three days or a week.

6. RESULTS AND DISCUSSION

Table 5 shows mining share in 24 hours for every currency. These are the mining incentive for each currency and each GPU card. These are net earnings, and have been subtracted with mining pool fee, transfer fee to the wallet, and other fees.

In high-end GPU section, the 1080Ti is leading as the top earner for five coins, while the RX Vega 64 outperform the 1080Ti in Ethereum, Monero, and FeatherCoin. However, this share is in its respective currency and must be converted to USD using the exchange rate valid for that time.

Both high end GPU consumes a lot of energy. The RX Vega 64 consumes the most energy when mining Ethereum (Ethash), Monero (Cryptonight), Bitcoin Gold (Equihash) and Verge (X17), while the 1080Ti consumes the most energy when while mining Siacoin (Blake2b), Decreed (Blake256), MonaCoin (Scrypt) and Feather Coin (Lyra2rRev2).

Table *6* shows the system energy used by each GPU to mine specific GPU.

Table 5: Mining Share in 24hrs

Coin	Mining Share in 24hrs			
	GTX 1080Ti	GTX 1070	RX Vega 64	RX 570
ETH	0.00184	0.00156	0.00224	0.00102
XMR	0.0046576	0.003109	0.0077344	0.0022574
BTG	0.0642911	0.0402726	0.0416773	0.0271428
XVG	37.684888	24.368461	17.748841	6.6081782
SC	0.78	0.45	0.52	0.26
DCR	0.0008876	0.0005159	0.0006623	0.0003094
MONA	0.5055446	0.2833796	0.0020623	0.0150502
FTC	3.2072956	2.1852923	4.7615279	2.1000724

The system (main board, excluding the external GPUs) consumes energy about 70 watts (1.68 kWh). Electric cost was calculated using the Indonesia electric rate, which equivalent to USD 0.11. Revenue (Rev) for each cryptocurrency and each GPU is calculated by multiplying shares in 24 hours (S) and exchange rate of the coin (Ex). The result is subtracted from energy cost, which is the energy consumption of the system in 24 hours (Ws) multiplied by the cost per kWh.

$$Rev = (S * Ex) – (Ws * 0.11) \quad (1)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 6: System Energy Consumption

Coin	System Energy Consumption in 24hrs (kWh)			
	GTX 1080Ti	GTX 1070	RX Vega 64	RX 570
ETH	5.95	4.82	6.82	3.36
XMR	4.54	3.58	6.24	3.44
BTG	6.72	5.64	6.96	4.9
XVG	5.95	6.67	6.96	4.2
SC	7.58	5.98	6.94	5.4
DCR	7.63	5.78	6.96	5.41
MONA	7.85	5.52	6.84	3.17
FTC	7.68	7.2	6.94	6.3

Table 7 shows detailed revenue for each cryptocurrency and each GPU.

Table 7: Revenue in 24hrs

Coin	Rate	Revenue in 24hrs (USD)			
		GTX 1080Ti	GTX 1070	RX Vega 64	RX 570
ETH	$703.4	$0.64	$0.57	$0.83	$0.35
XMR	$201.7	$0.44	$0.23	$0.87	$0.08
BTG	$44.44	$2.12	$1.17	$1.09	$0.67
XVG	$0.03	$0.30	($0.12)	($0.32)	($0.29)
SC	$0.02	($0.82)	($0.65)	($0.75)	($0.59)
DCR	$89.96	($0.76)	($0.59)	($0.71)	($0.57)
MONA	$3.30	$0.81	$0.33	($0.75)	($0.30)
FTC	$0.10	($0.53)	($0.58)	($0.30)	($0.49)

Table 7 shows that from 32 sets of experiment, only 15 sets (46.88%) are profitable. From eight coins tested, the 1080Ti GPU is profitable at five coins (62.5%), followed by the GTX 1070 at four coins (50%), RX Vega 64 and RX 570 at three coins each (37.5% each). Although the RX Vega 64 is ranked above the 1070, the later GPU is more profitable in more coins, since it consumes lower energy.

Note that the revenue is calculated without including air conditioning costs. Table 8 also shows that all GPU generates heat more than 40°C, which gradually raise the room temperature. In the long time mining process, air conditioning would be mandatory, not only to make the room comfortable for people, but also such high temperature could damage the hardware. The design of the Vega 64, which only have one fan and closed heatsink design, is also contributing to its highest temperature.

Table 8: Average GPU Temperature

Coin	Average GPU Temp (C)			
	GTX 1080Ti	GTX 1070	RX Vega 64	RX 570
ETH	57	58	70	58
XMR	50	50	65	58
BTG	61	59	75	59
XVG	62	57	60	57
SC	63	66	63	58
DCR	57	61	65	59
MONA	64	61	46	57
FTC	56	64	67	59

Table 9 shows best performer GPU for every coin, which calculated by how much power consumption needed to produce one mega hash.

Table 9: Best Performer GPUs

Coin	Best Performer GPU in terms of W/MH)	Power (W) per hash rate (MH)
ETH	RX 570	4.837260728
XMR	RX Vega 64	158333.3333
BTG	GTX 1080Ti	313493.6629
XVG	GTX 1080Ti	9.621621622
SC	GTX 1080Ti	0.094506339
DCR	GTX 1070	0.066276501
MONA	GTX 1080Ti	4.644018793
FTC	RX Vega 64	116.3506074

Given the global network hash rate for every coin at the time, we calculate the power required to run the network for each coin, and the estimated annual energy consumption, as detailed in Table 10.

Table 10: Estimated Annual Energy Consumption for the Coin Network

Coin	Network Hash Rate (MH/s)	Power Required (MW)	Est. Annual Energy Consumption (TWh)
ETH	270,385,640.00	1,307.93	11.46

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Coin	Network Hash Rate (MH/s)	Power Required (MW)	Est. Annual Energy Consumption (TWh)
XMR	452.26	71.61	0.63
BTG	30.48	9.55	0.08
XVG	551,700.00	5.31	0.05
SC	73,189,400,000.00	6,916.86	60.59
DCR	17,033,750,000.00	1,128.94	9.89
MONA	2,040,000.00	9.47	0.08
FTC	10,126.82	1.18	0.01

As a comparison, Bitcoin estimated annual energy consumption in June 8th, 2018 was 70.842 TWh [6]. Most of the coins above have a significant power consumption gap below the Bitcoin. However, in cryptocurrency, mining is permissionless, and the price of the coin depends entirely on supply and demand. When a coin attracts too many miners (or when miners use ASIC, which can produce a very high hash rate at lower power consumption), the blockchain automatically adjusts the difficulty to maintain constant block time. High network hash rate creates a barrier for miners. Miners with lower hash rate will receive less incentive, and they will likely exit the system because it is not profitable anymore. Less miners in the system (also ASIC owners) lead to less decentralized system, and it is not desirable.

Table 11: Daily Energy Cost

Coin	Market Capitalization (Million US$)	Daily Energy Cost (Million USD)	% Energy Cost/Market Cap.
BTC	$130,256.22	$21.3496	0.016%
ETH	$69,465.82	$3.4529	0.005%
XMR	$3,237.59	$0.1890	0.006%
BTG	$770.34	$0.0252	0.003%
XVG	$381.54	$0.0140	0.004%
SC	$574.99	$18.2605	3.176%
DCR	$642.84	$2.9804	0.464%
MONA	$197.69	$0.0250	0.013%
FTC	$19.54	$0.0031	0.016%

Table 11 shows daily energy cost of running each coin compared to Bitcoin. The data are taken from the testing date, except the Bitcoin from June 8th, 2018. Energy cost is calculated based on Indonesia electricity cost. From the table, we can observe that even the energy consumed by the SiaCoin network is lower than Bitcoin, but the energy consumption proportion to market capitalization is 19,276% more than Bitcoin. At some point, coin developers have to take drastic actions. For example, the SiaCoin decided to perform hard fork to reset its PoW algorithm on October 31. The reset restricts ASICs such as Innosilicon and Bitmain [36], and push down the network hash rate to 932.70 TH/s by November 5.

For miners, calculating profitability can be complicated, since coin price depends heavily on the price of bitcoin, and the price of bitcoin is very sensitive to cryptocurrency issues and policies. During the testing period, Bitcoin price reaches its peak at USD 8,454.75 on May 21, and drops to USD 5,954.43 on June 29 before climbing back to USD 7,000s. To describe its volatility, the Bitcoin highest price was USD 19,747.87 on December 17, 2017 [37].

The use of blockchain in cryptocurrency may significantly reduce the need for banks, which could lower the transaction fee to a minimum, but the PoW base blockchain runs on miners, and with the amount of energy required, daily cost to maintain a coin could reach millions of dollars.

7. CONCLUSIONS

The PoW system relies on miners to run the system. Our experiment shows only 46.88% of 32 sets are profitable. Equihash, Ethash, and Cryptonight7 coins are the best performers, while Blake2b, Blake256, and Lyra2REv2 coins are the worst performers in terms of profitability. Most the coins tested consume below than 1 TWh ($110,000,000.00) of annual electrical energy consumption, except SiaCoin and Ethereum, and Decred.

Higher profitability means miner will probably continue to contribute to the system. Profitability also depends on the exchange rate of the currency, which rely heavily on the BTC exchange rate. To make it more complicated, cryptocurrencies price solely depends on supply, demand and the expectation of the holder. No central bank, government, nor anybody can correct the price should it rises or fall. Because the permissionless nature of the blockchain, miners can easily switch to mine more profitable coin. Actions such as hard fork, switching algorithm or even switching consensus mechanism is common in the cryptocurrency world. This makes public, permissionless blockchain which runs on PoW has a high level of uncertainty.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

REFRENCES:

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[2] CoinMarketCap, "All Coins," [Online]. Available: https://coinmarketcap.com/coins/views/all/. [Accessed 7 July 2018].

[3] M. V. Alstyne, "Economic and Business Dimentions; Why Bitcoin Has Value," Communications of the ACM, 2014.

[4] Z. Z. Sun, S. X. Sun and H.-N. D. Macau, "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services,* no. December, 2017.

[5] K. J. O'Dwyer and D. Malone, "Bitcoin Mining and its Energy Footprint," in *5th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communities Technologies (ISSC 2014/CIICT 2014)*, 2014.

[6] Digiconomist, "Bitcoin Energy Consumption Index," [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption. [Accessed 11 December 2018].

[7] S. Deetman, "Bitcoin Could Consume as Much Electricity as Denmark by 2020," Vice: Motherboard, 29 March 2016. [Online]. Available: https://motherboard.vice.com/en_us/article/aek3za/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020. [Accessed 11 July 2018].

[8] F. Flipo and M. Berne, "The bitcoin and blockchain: energy hog," The Conversation, 17 May 2017. [Online]. Available: http://theconversation.com/the-bitcoin-and-blockchain-energy-hogs-77761. [Accessed 11 July 2018].

[9] C. Malmo, "A Single Bitcoin Transaction Takes Thousands of Times More Energy Than a Credit Card Swipe," Vice: Motherboard, 8 March 2017. [Online]. Available: https://motherboard.vice.com/en_us/article/ypkp3y/bitcoin-is-still-unsustainable. [Accessed 11 July 2018].

[10] M. Dobrovnik, D. M. Herold, E. Fürst and S. Kummer, "Blockchain for and in Logistics: What to Adopt," *Logistics,* vol. 2, no. 18, 2018.

[11] A. Sivula, A. Shamsuzzoha and P. Helo, "Blockchain in Logistics: Mapping the Opportunities in Con-struction Industry," in *International Conference on Industrial Engineering and Operations Management*, Washington. D.C., 2018.

[12] Institute for Austrian and International Tax Law, "Blockchain: Taxation and Regulatory," 2017.

[13] Delloite, "Blockchain technology and its potential in taxes," 2017.

[14] C. Henly, S. Hartnett, S. Mardell, B. Endemann, B. Tejblum and D. S. Cohen, "Energizing The Future With Blockchain," *Energy Law Journal,* vol. 39, no. 197, 2018.

[15] M. Hölbl, M. Kompara, A. Kamišalic and L. N. Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," *Symmetry,* vol. 10, no. 470, 2018.

[16] I. Radanović and R. Likic, "Opportunities for Use of Blockchain Technology in Medicine," *Applied Health Economics and Health Policy,* vol. 16, no. 5, 2018.

[17] G. J. Katuwal, S. Pandey, M. Hennessey and B. Lamichhane, "Applications of Blockchain in Healthcare: Current Landscape & Challenges," 2018.

[18] A. Kumar and C. Smith, "Crypto-currencies – An introduction to not-so-funny moneys," Reserve Bank of New Zealand, November 2017.

[19] A. Berentsen and F. Schär, "A Short Introduction to the World of Cryptocurrencies," Federal Reserve Bank of St. Louis Review, First Quarter 2018, 2018.

[20] Merriam-Webster, "Currency," [Online]. Available: https://www.merriam-webster.com/dictionary/currency. [Accessed 26 June 2018].

[21] W. H. Furness, The Island of Stone Money, J.B. Lippincott Company, 1910.

[22] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *IEEE 6th International Congress on Big Data*, 2017.

[23] S. Hameed and S. Farooq, "The Art of Crypto Currencies," *International Journal of Advanced Computer Science and Applications,* vol. 7, no. 12, 2016.

[24] I. Eyal and E. G. Sirer, "Majority is not Enough: Bitcoin Mining is Vulnerable," in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The Twelfth Workshop on the Economics of Information Security (WEIS 2013), 2013.

[25] Electroneum, "Electroneum Overview & White Paper".

[26] M. Rudlang, "Comparative Analysis of Bitcoin and Ethereum," Norwegian University of Science and Technology, 2017.

[27] Seigen, M. Jameson, T. Nieminen, Neocortex and A. M. Juarez, *CryptoNight Hash Function,* CryptoNote, 2013.

[28] A. Biryukov and D. Khovratovich, "Equihash: Asymmetric Proof-of-Work Based," *Ledger,* vol. 2, pp. 1-30, 2017.

[29] E. Duffield and D. Diaz, "Dash: A Payment-Focused Cryptocurrency," 2014.

[30] J.-P. Aumasson, S. Neves, Z. Wilcox-O'Hearn and C. Winnerlein, "BLAKE2: simpler, smaller, fast as MD5," 2013.

[31] C. Percival and S. Josefsson, "The scrypt Password-Based Key Derivation Function," Request for Comments: 7914, 2016.

[32] S. J. Marcos A., L. C. Almeida, E. R. Andrade, P. C. F. d. Santos and P. S. L. M. Barreto, "Lyra2: Efficient Password Hashing with High Security against Time-Memory Trade-Offs," *IEEE Transactions on Computers,* vol. 65, no. 10, pp. 3096 - 3108, 2016.

[33] Blockchain Luxembourg S.A., "Hashrate Distribution," [Online]. Available: https://www.blockchain.com/pools?timespan=48hours.

[34] CoinMarketCap, "Top 100 Cryptocurrencies By Market Capitalization," 13 March 2018. [Online]. Available: https://coinmarketcap.com/. [Accessed 13 March 2018].

[35] Notebook Check, "Mobile Video Graphics Cards - Benchmark List," [Online]. Available: https://www.notebookcheck.net/Mobile-Graphics-Cards-Benchmark-List.844.0.html. [Accessed 30 August 2018].

[36] Nebulous, Inc., "Navigating the Sia hardfork," [Online]. Available: https://support.sia.tech/article/kwadovujkr-sia-fork-nov-1-2018#hardfork_is_implemented. [Accessed 15 December 2018].

[37] Cointelegraph, "Bitcoin Price Index," [Online]. Available: https://cointelegraph.com/bitcoin-price-index. [Accessed 20 August 2018].

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195