Cryptocurrency Mining – Transition to Cloud

Hari Krishnan R.1
Department of Computer Science and Engineering
SRM University, Chennai, India

Sai Saketh Y. 2
Department of Computer Science and Engineering
SRM University, Chennai, India

Venkata Tej Vaibhav M.3
Department of Computer Science and Engineering
SRM University, Chennai, India

***Abstract*—Cryptocurrency, a form of digital currency that has an open and decentralized system and uses cryptography to enhance security and control the creation of new units, is touted to be the next step from conventional monetary transactions. Many cryptocurrencies exist today, with Bitcoin being the most prominent of them. Cryptocurrencies are generated by mining, as a fee for validating any transaction. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs and ASICs, running complex hashing algorithms like SHA-256 and Scrypt, thereby leading to faster generation of cryptocurrencies. This arms race for cheaper-yet-efficient machines has been on since the day the first cryptocurrency, Bitcoin, was introduced in 2009. However, with more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest huge sums of money on employing multiple high performance ASICs. Thus the value of the currency obtained for finding a hash did not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the enormous amount of heat they produce and electricity required to run them. The next logical step in this is to utilize the power of cloud computing. Miners leasing super computers that generate hashes at astonishing rates that have a high probability of profits, with the same machine being leased to more than one person on a time bound basis is a win-win situation to both the miners, as well as the cloud service providers. This paper throws light on the nuances of cryptocurrency mining process, the traditional machines used for mining, their limitations, about how cloud based mining is the logical next step and the advantage that cloud platform offers over the traditional machines.**

Keywords*—*Cryptocurrency; Bitcoin mining; Cloud mining; Double Spending; Profitability

I. Introduction To Mining

Mining is the integral process wherein generation, transmission and validation of transactions of cryptocurrencies is done. It ensures stable, secure and safe propagation of the currency from the payer to payee. Unlike fiat currency, where a centralized authority controls and regulates the transactions, cryptocurrencies are decentralized and work on a peer-to-peer system. Banks that generate physical currency and monitor the transactions require huge infrastructure to function and operate. Cryptocurrencies overcome this need by implementing a mining system where people in the network, called 'miners' or 'nodes', monitor and validate transactions which generates currency.

In cryptocurrency, a transaction is a transfer of coins from one wallet to another. When a transaction is made, the details of the transaction will be broadcast to every node in the network. The transactions made over a set period of time are collected to form a 'Block'. To incorporate transparency in the system, it is designed in such a way that all the transactions made from the inception of the currency are recorded and maintained in a general ledger called the 'Block chain' which, as the name suggests, is a list of blocks created from the beginning.

Miners play a predominant role in mining. Miners process transactions by verifying the ownership of the currency from source to destination. Every transaction contains the hash of the previous transaction made by the owner through which authenticity of a present transaction is tested, thereby validating it. Miners also inhibit double spending of the currency through this validation process.

The main purpose of mining is to generate and release coins into its coin economy. Whenever a transaction takes place and is validated, miners collect these transactions and include them into the block they are currently solving. Every block has to be solved before being broadcasted and put in the block chain. Solving of a block involves mathematical puzzles which are difficult to unlock and crack provided there will be some constraints on the output generated. Only on solving the mathematical puzzle is one allowed to add the block to the ledger and a reward of coins is given in return. Thus mining eventually boils down to a competition of mathematical puzzles to solve for the reward of coins. This mechanism prevents miners from easily procuring coins and thus maintains the fairness of the system. [1][2][3][4]

II. Mining Machines

Mining of crypto currency is done through purpose specific designed machines called as 'Mining machines'. The history of mining machines starts from CPU to the currently widely used ASICs. The periodic growth of mining difficulty led to evolution of new machines with higher efficiency than previously designed machines. The cost and performance of the mining machine determine its mining profitability, hence the design and its implementation is very crucial in mining. The various machines used in mining are:

A. CPU

During initial days of mining, CPU was used to mine the coins effectively with hash rates less than or equal to 10MH/sec. A personal PC with mining software installed in it was enough to cope with the mining process. But, due to the constant increase of difficulty in mining, usage of CPU's as mining machine became irrelevant to the evolving machines with higher hashing rates. A popular mining software for CPU mining was cpuminer.

cpuminer is a simple client program that performs Pooled Mining or solo mining. The program receives proposed block data from the server, for which it tries to guess a nonce value that will result in a valid block. If a block hash with at least 32 consecutive zero bits is found, the block data containing the guessed nonce value is sent back to the server. If used in Pooled Mining mode, this block is called a "share" because the server is supposed to credit the registered user's account, according to the number of shares that user has contributed, and eventually transfer an amount of Bitcoins to the registered user's address.

B. GPU

As the power of CPU mining didn't meet the growing demands, CPU with Graphic cards are used to mine the coins. Graphic cards contain Graphical Processing Units (GPU's), which are used to solve high mathematical calculation functions and complex polygons used in gaming. Different cryptocurrencies uses different hash-proof based algorithms to solve transaction blocks which require high mathematical lifting, hence GPU's were seen as a credible alternative to the CPU mining.

A CPU core can execute 4 32-bit instructions per clock (using a 128-bit SSE instruction) or 8 via AVX (256-Bit), whereas a GPU like the Radeon HD 5970 can execute 3200 32-bit instructions per clock (using its 3200 ALUs or shaders). This is a difference of 800 (or 400 in case of AVX) times more instructions per clock. As of now, the fastest CPUs have up to 6, 8, or 12 cores and a somewhat higher frequency clock (2000-3000 MHz vs. 725 MHz for the Radeon HD 5970), but one HD5970 is still more than five times faster than four 12-core CPUs at 2.3GHz (which is also costlier at $4700 when compared to $350 for the HD5970).

In October 2010 an open-source OpenCL miner was released on the web which was rapidly optimized and adapted by miners. These miners would typically implement the SHA protocol in languages such as Java or Python which was compiled down by the hidden ISA of the GPU.

Since these rigs are left to mine for many months the users aggressively tweak the voltages (to lower in order to reduce mining costs, or higher, with frequency, to increase Gh/s) and operating frequencies of video ram (lower to save energy, since memory is unused) and the GPU core itself, as well as parameters of the code such as the number of threads that are enqueued at a given instance, so as to maximize throughput within reasonable bounds of stability and temperature. Since the Bitcoin computation does not exercise the memory system, many of the critical paths and bottlenecks in the GPU are not exercised, which means that the system can be pushed beyond the normal bounds of reliability. Over time it often becomes necessary to retune the parameters as fans and power delivery system wear eventually causes the GPU core to run too slowly.

GPUs tend to be much more accessible than FPGAs for end users, requiring PC-building skills and avid forum reading but no formal training in parallel programming or FPGA tools. The goal of scaling BTC hash rate through GPUs pushes the limits of consumer computing in amazing and novel ways. Despite such benefits GPU have some limitations.

Limitations:

- Though Graphic cards can give over 800 MH/sec, but they are of high cost than normal CPU's.
- The GPUs cannot be used standalone. Each GPU has to be plugged into a PCI-E 8x or 16x slot, of which there are relatively few on commercial motherboards.
- All the components like motherboard, hard-drive and RAM are not used in GPU mining which ultimately increases the cost of mining.
- GPU's require high additional power of 200-300W for mining effectively.
- GPU's normally takes two slots in a case or motherboard which makes it difficult to attach two or more GPU's to a single computer for greater performance.

GPU mining is largely inactive these days as the mining difficulty has exceeded the levels it can compete and further, with the advent of FPGAs and ASICs into the field of mining which vouched for good mining profitability.

C. FPGA (Field Programmable Gate Array)

June 2011 brought the first open-source FPGA Bitcoin miner implementations. With the constant increase of mining cost against the coins earned as a result of mining, it impacted mining profitability in a negative sense. GPU mining with its high mining cost and low $ per day return was incompetent to mine any more. There was an immediate need for an emergence of machines which could make the mining profitable for the miners to continue with the mining.

FPGA known as Field Programmable Gate Array is a reprogrammable IC which can be configured or designed after manufacturing. FPGAs contain individual programmable logic blocks commonly called as Configurable Logic Blocks (CLB). These logic blocks are inter-connected in a manner that can be reconfigured. FPGAs contain large resources of logic gates and RAM's for complex digital computation.

FPGAs are flexibly configurable and reprogrammable, hence a designer can design and implement any digital function. FPGAs are easier to synthesize than its other counterparts which made FPGAs a good option for Bitcoin mining. FPGAs are reusable as they can be reprogrammed very easily. FPGAs consume energy one-fifth less than that of GPU, which was a major issue with GPU mining. FPGAs are also good at rotate-by-constant operations and at bit-level operations used in hash-proof based algorithms like SHA256 used in Bitcoin transactions.

A Butterfly labs mini rig FPGA mines at around 25,200Mh/s with efficiency 20.26Mhash/J consuming 1,250Watts of power I contrast to the GPU's which mine at 800MH/s in general.

Limitations:

- Though BTC FPGAs are easily synthesizable, they consume high power than typical FPGAs.
- FPGAs are good for low quantity production, otherwise cost per product increases with the required quantity increment which less efficient than its competitors like ASICs.

D. ASIC (Application Specific Integrated Circuit)

Mining coins with time became hard to come by with the upgraded machines available at cheaper prices made huge competition among the miners to achieve more gains through mining. FPGAs designed for mining purpose though are flexible to program and manufacture, consumes a lot of power against the return it gets. With the use of ASICs for mining, these offered an improved performance than FPGAs when used for large scale mining. ASICs are a logical progression of this trend: circuits are specifically designed to calculate hashes as fast as possible, while consuming as little energy as possible. The best ASICs on the market today are capable of well over 1,000 Mhash (1 billion hashes) per joule of energy.

ASICs are Application Specific Integrated Circuits used for various types of specified applications. They are microchips built for single purpose though its applications are implemented in various fields. Bitcoin ASICs which are designed specifically to mine Bitcoins, are good at complex mathematical tasks that mining needs, as fast and efficiently as possible. Although FPGAs dominated only a short time, its development efforts served as a quick stepping stone to ASICs. ASIC Verilog are similar to FPGA Verilog in its design and implementation that came before it.

Advanced ASICs in the present market are capable of producing more than or equal to 1,000Mhash per joule of energy consumed. An ASIC Ant-Miner S5 costing up to $370 typically gives 1957Mhash/J and consumes around 590 Watts, which makes ASICs the most profitable privately owned machine available in the market for mining as of today.

The disadvantages faced through ASICs is its cost and the speed with which the entire field is developing. The pace with which the field is updating with improved hardware achieving high hash rates than previously designed economically makes the ASIC mining profitable only for a short period of time until a new machine with higher performance emerges.

Due to its obvious advantages when compared to the other mining machines available, ASICs are currently reigning the mining field with their performance, though it remains to be seen how much it will withstand and sustain with the ever emerging improved machines. [2][8]

III. Comparison of Hardware

Mining machines characterize the whole mining process with their action and output. Mining difficulty and mining profitability are dependent on the machines used at the respective times in the history of mining. Figure 1 shows the revenue per GH/s that bit coin network generated since 2010. The horizontal lines depict the energy costs per GH/s of CPU'S, GPU'S, FPGAS and ASICS. When revenue per GH/s goes below these costs the profits will turn negative and rig should turn off.

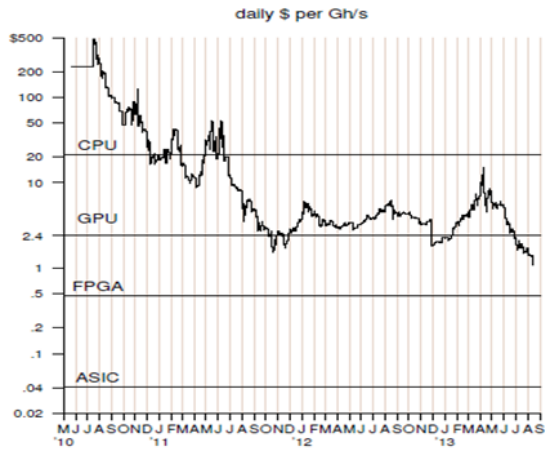

Fig. 1. Revenue per GH/s vs. Energy costs [8]

The above graph also suggests that ASICs have the highest returns/capital spent on energy requirement in comparison to the other three mining systems.

The general comparison between ASICs, FPGAs, GPUs and CPUs against various parameters is shown below:

TABLE I. Performance Characteristics of Various Machines [9]

NAME	TYPE	HASH RATE 'R' (Mhash/S)	POWER 'P' (WATTS)	ENERGY EFFICIENCY 'E' (Mhash/J)	COST ($)
CORE i7 950	CPU	18.9	150	0.126	350
Atom N450	CPU	1.6	6.5	0.31	169
ATI 4850	GPU	101.0	110	0.918	45
ATI 5770	GPU	214.5	108	1.95	80
DIGILENT NEXYS 2 500K	FPGA	5.0	5.0	1	189
MONARCH BPU 600 C	ASIC	600000.0	350	1714	2196
BLOCK ERUPTER SAPPHIRE	ASIC	333.0	2.55	130	34.99

IV. Profitability

Profitability is a major criterion when we consider performing Bitcoin mining operations. The profitability of mining depends on factors like:

- The initial cost of the mining rigs like the ASICs
- The hashing rate of the machine
- The total network hashing power and the current difficulty of hashing problems.
- The cost of electricity consumption.
- The current and future value of Bitcoins.

A traditional mining technique requires miners to purchase large and multiple highly powered ASICs machines to

perform hashing operations which yields Bitcoins. However such a technique is not practical to a new or even an experienced miner with respect to profitability. This is because as the number of miners increases, greater amount of processing power is being added to the Bitcoin network. This requires vast amount of electricity to keep the machines running at constant rate and thereby not only resulting in a higher carbon footprint that has environmental consequences but also increasing the cost of electricity consumption per machines, thereby reducing the profit obtained by mining of Bitcoins.

A. *Efficiency calculations*

Mining requires a lot of electricity. If we are building a DIY system then we will be getting an ATX power supply unit (PSU). Therefore it's worth investing in the most efficient supply you can get.

Let us consider the following two cases for determining efficiency of rigs: A PSU that is guaranteed to supply 860W and is 93% efficient would actually draw 925W (860W/0.93). By contrast, a 750W power supply that is only 80% efficient would actually draw 937.5 W (750/0.8) - thus using more power, but supplying less. When building a mining rig, miners will need to take account of the power requirements of all the components they are using, especially all the graphics cards. Also it is a good idea to provide some excess capacity to deal with unexpected events and provide the potential to overclock the system. ASICs, on the other hand, can do far more calculations with far less power because they are highly specialized devices. And since they ship with an appropriate power adapter, miners do not have to worry about doing all the math to find one that is up to the task. The mining efficiency of different systems can be compared by taking the ratio of the number of hashes it can perform in a second, divided by the power it consumes:

Hashing speed / power consumption = mining efficiency.

The profitability calculators like the Genesis block ask for the electricity costs and the initial investments in the hardware. Effectively the miners are being asked for their ongoing and one-off investments. The conversion process isn't completely straightforward; In the case of hardware miners, the monthly running cost can be worked out by multiplying the electricity charge (i.e., $ per KWh) by the power consumption of the unit and by a conversion factor of 0.744 (the ratio of seconds per month to joules of energy per KWh).

However the main question is: Has profitability increased or decreased over the years?

Recent data, table 2, pertaining to difficulty of mining and corresponding hash rates clearly indicate that traditional mining techniques can lead to losses or reduce profitability substantially. From the data we can conclude that over period of 11 months the difficulty and hashing rate has increased by 7.5% and 346.81331% respectively. Additionally, there is not guarantee that the value of Bitcoins and other cryptocurrencies will remain stable or even rise. Speculations and increasing regulation constantly encourage different parties to join in or exit the market. While the picture is one of increasing adoption, major developments can still affect the price markedly.

TABLE II. BITCOIN DIFFICULTY AND HASH RATE HISTORY (11 MONTHS) [25]

Date	Difficulty	Change	Hash Rate
Mar 22 2015	46,717,549,645	-1.50%	334,417,246 GH/s
Mar 08 2015	47,427,554,951	1.59%	339,449,662 GH/s
Feb 22 2015	46,684,376,317	5.01%	334,179,783 GH/s
Feb 09 2015	44,455,415,962	7.71%	318,224,263 GH/s
Jan 27 2015	41,272,873,895	-6.14%	295,442,739 GH/s
Jan 12 2015	43,971,662,056	8.20%	314,761,417 GH/s
Dec 30 2014	40,640,955,017	3.00%	290,919,288 GH/s
Dec 17 2014	39,457,671,307	-1.37%	282,449,013 GH/s
Dec 02 2014	40,007,470,271	-0.73%	286,384,627 GH/s
Nov 18 2014	40,300,030,328	1.76%	288,478,854 GH/s
Nov 05 2014	39,603,666,252	10.05%	283,494,086 GH/s
Oct 23 2014	35,985,640,265	2.81%	257,595,247 GH/s
Oct 09 2014	35,002,482,026	0.98%	250,557,526 GH/s
Sep 25 2014	34,661,425,924	16.20%	248,116,151 GH/s
Sep 13 2014	29,829,733,124	8.75%	213,529,547 GH/s
Aug 31 2014	27,428,630,902	15.03%	196,341,788 GH/s
Aug 19 2014	23,844,670,039	20.86%	170.686.797 GH/s
Aug 08 2014	19,729,645,941	5.30%	141.230.307 GH/s
Jul 25 2014	18,736,441,558	8.08%	134.120.673 GH/s
Jul 12 2014	17,336,316,979	3.08%	124,098,191 GH/s
Jun 29 2014	16,818,461,371	24.93%	120,391,236 GH/s
Jun 18 2014	13,462,580,115	14.51%	96,368,902 GH/s
Jun 05 2014	11,756,551,917	12.44%	84,156,677 GH/s
May 24 2014	10,455,720,138	18.10%	74,844,960 GH/s

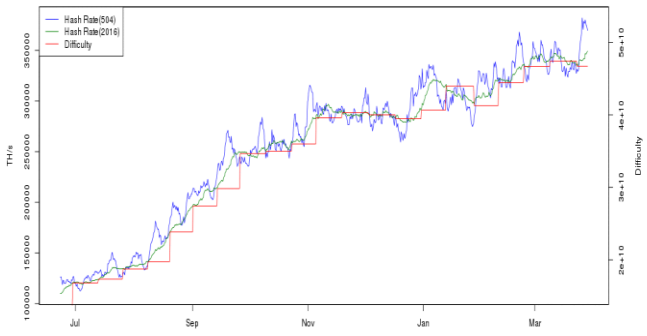

Fig. 2. Bitcoin Hash Rate vs Difficulty (9 months)

V. ISSUES IN TRADITIONAL MINING

A. Double spending problem

Double spending as the name goes suggests is a successful spending of a money more than once. Double spending is a unique problem associated with digital currencies because the digital data can be reproduced easily unlike physical currency.

Crypto currency network involves mining which is a Proof of Work (PoW) based. Users do the transactions by digitally signing their transactions over the network through a distributed time stamp service to prevent double spending of coins. In double spending, any digital currency holder can make a copy of the currency and might send it to any merchant or any other party while retaining the original.

For example, a popular digital currency like Bitcoin takes an average 10 to 15 minutes for conformation of a transaction and which is why is not efficient for fast payments. But this process is essential for the detection of double spending of coins. Since all digital currency users are anonymous and hold multiple accounts, it is practically very difficult to trace out the fraudsters. This problem was acknowledged by the Bitcoin developers and suggested a mechanism such that merchants don't have to wait for the conformation if the transaction amount is not a huge sum. But this proposal doesn't remove the double spending problem of the network theoretically since Bitcoin is increasingly used in fast payments like ATM transaction, restaurant bills etc…

Understanding the conditions for double spending needs a knowledge about the types of payments involved in digital currencies. Generally, two types of payments namely slow and fast payments are present.

Slow Payments: Slow payments are the conventional way of transaction mechanism. Slow payments are accepted after the conformation of the transaction by the network. Since confirmed transactions are accepted by the honest peers, any malicious attempts will have negligible advantage.

The study shows that 64% of the transactions in Bitcoin network are confirmed under or below 10 min whereas remaining 36% took 10-40 min time for conformation.

Fast Payments: When payments are done in a quick time, they cannot operate on the basis of conformations of the transactions like supermarkets, vending machines etc…These kind of payments comes under fast payments where exchange of currency and goods are done in a shorter time.

In Bitcoin transactions to enable faster payments, merchants are suggested to approve the transaction without any conformation if it's not of a higher value. But the measure can't avoid the vulnerability of the Bitcoin network.

Necessary conditions for successful Double-spending:

To successfully double spend the money, the attacker needs to make the vendor accept the transaction (TRv) that will not be redeemed afterwards. An attacker creates a transaction (TRa) which will have same inputs as TRv but the recipient address will be an address which under his control or any other vendor or merchant.

The conditions which help an attacker to have a successful double-spending are:

- When the time taken by the vendor to accept the transaction TRv is less than the time taken by vendor to acknowledge the transaction TRa. Since network doesn't support multiple transactions that share common inputs, the transaction TRv cannot be redeemed.
- When the transaction TRa is already confirmed in any other block, then the transaction TRv is never confirmed by the network.

Types of attacks:

- Race Attack: Immediate acceptance of a 0/unconfirmed transaction by the vendor or the merchant leads to race attack. The coins in the transaction showed to the merchant might have been used in different transaction that would be first to make into the block. So, the transaction done to the merchant by the attacker has high chances of getting rejected and cannot be redeemed by the merchant.
- Finney Attack: Finnely attack is a fraudulent double-spending which requires the participation of a miner. A miner will have to include a non-broadcasted transaction which is deceiving in his block generation to achieve double-spending. But this attack is irrelevant for a smaller amounts and will not make any profit for the risk involved in it.
- >50% attack: When the attacker maintains or controls more than 50% of the network hash rate then this attack is possible. So, there will be higher chances of making a false transaction getting conformed across the network. Only high profits can make an attacker to resort to such an attack but since the mining is gaining popularity day by day it becomes practically impossible now.

Though, double-spending is theoretically possible, practically only a negligible amount of fraud is done through this mechanism. Now-a-days much of the fraud is done due to the insecurity of the wallets present at each node.

B. Malware

Malware, also called ransom-ware, is a hacker-controlled bot-net that directly attacks the PC or encrypts files stored in the drives. A type of such malware is 'Trojan-Ransom.Win32.Linkup' which blocks the internet access by modifying the DNS and turning the computer into a Bitcoin mining bot at the same time.

In addition to messing around with the DNS, Linkup can also link up to a remote server and pressgang the PC into service as a Bitcoin-mining bot. This is carried out via a downloader called 'pts2.exe', which extracts a second file, named 'j.exe', onto a computer. This is, in fact, a popular piece of mining software called 'jhProtominer'.

The damage that is likely to be inflicted by the Trojan is limited. jhProtominer only works on 64-bit operating systems,

but even so, it still leaves plenty of computers around the globe to infect.

How do does the malware (also miners) get into mining systems?

BKDR_BTMINE.MNR may arrive on users' systems as part of a malware package. It may either be dropped or downloaded by other malware/ grayware/spyware from malicious sites. These may also be unknowingly downloaded by users while visiting malicious sites. BKDR_BTMINE.DDOS may also arrive as part of a malware package. These may be downloaded by other malware/grayware/ spyware from malicious sites or may be unknowingly downloaded by users while visiting malicious sites. Cybercriminals use social media to infect users' systems with Bitcoin-mining malware. They have, for instance, used Tweets with malicious links to trick users into downloading WORM_KOLAB.SMQX, which subsequently download HKTL_BITCOINMINE onto infected systems. Some cybercriminals also used WORM_OTORUN.ASH to exploit a certain network vulnerability to force systems to participate in a Bitcoin pool. It may also be dropped or downloaded by other malware/spyware/ grayware from malicious sites.

What happens to Bitcoin-mining-infected systems?

Bitcoin-mining malware primarily aim to force systems to generate Bitcoins for cybercriminals use.

BKDR_BTMINE.MNR accesses malicious URLs to procure certain IP addresses. It then accesses the IP addresses to send and receive information, to download other malware, and to get an updated list of IP addresses. It also downloads and uses one of three different Bitcoin-mining software, depending on the infected system's specifications.

BKDR_BTMINE.DDOS comes with a list of IP addresses that it tries to access in order to send and receive information, to download other malware, to get an updated list of IP addresses, and to obtain a list of sites to target via distributed denial-of-service (DDoS) attacks. Upon execution, WORM_KOLAB.SMQX creates a directory that contains HKTL_BITCOINMINE—a Bitcoin-mining-mining grayware, in an infected system. WORM_KOLAB.SMQX uses this grayware to generate Bitcoins without the users' knowledge. During analysis, the grayware tried but failed to access a malicious link using a specific user name and password. WORM_OTORUN.ASH attempts to force infected systems to participate in a Bitcoin-mining pool service known as Deepbit. A Bitcoin mining pool refers to a network of Bitcoin miners that process the same block for faster payout. The Bitcoins generated through such a pool are then divided among the participants.

C. Energy footprint

Bitcoin mining network is stuck in a cycle which is driving up its power usage. Miners tend to put more computing power on the network so that they can make more and more Bitcoins. The software underpinning the network reacts by changing a parameter that makes it more difficult to solve the mathematical problem needed to solve a Bitcoin block. Therefore, because it is harder to solve the problem, miners add even more computing power. As this cycle increases, it takes more electricity to mine a Bitcoin. The hashing power of the network surpassed the world's top 500 supercomputers almost a year ago. So the higher the value of one Bitcoin, the higher the value of mining rewards and transaction fees, the higher the energy consumption of the Bitcoin network in the long run.

Energy consumption and Bitcoin mining relation can be described as follows:

More efficient mining gear does not reduce energy use of the Bitcoin network. It will only raise the network difficulty

Cheaper energy linearly increases mining energy use of the Bitcoin network

The same conclusions apply to all proof of work based currencies.

A Bitcoin miner is part of Bitcoin's peer-to-peer network that collects recent transactions and aims to complete a proof of work scheme. In this scheme, there is a current target value T, which is periodically recalculated by the network. The miner's aim is to find a nonce value so that:

$$H(B.N) < T(1)$$

where B is the string representing the recent transactions, N is the nonce value, '.' is the concatenation operator and H is the Bitcoin hash function, in this case:

$$H(S) := SHA256\ (SHA256(S))$$

The proof of work can be achieved by choosing values for N randomly or systematically until eq.1 is satisfied. When an N is found, the resulting block can be sent to the Bitcoin network and added to the Bitcoin blockchain. Finding a block results in a reward of extra Bitcoins for the block's finder.

Thus, the process of finding a suitable N value is referred to as Bitcoin mining.

The major limiting factors in Bitcoin mining are the hash rate of hardware and the cost of running this hardware. The hash rate, R, is typically measured in millions of hashes per second or Megahashes (Mhash/s). This is combined with the power usage, P, of the hardware to get the energy efficiency of the hardware E = R/P (Mhash/J) which serves as a helpful statistic to compare hardware.

Initially mining took place on normal computers. As Bitcoin gained popularity, there was something akin to an arms race as miners attempted to increase their hash rate. Graphics Processing Units (GPUs) which can perform many parallel calculations are well-adapted to Bitcoin mining. Standard programming interfaces, such as OpenCL and CUDA, made GPUs popular among Bitcoin miners. Their higher hash rate compared with their lower energy footprint made them better suited to mining than normal CPUs. As the use of GPUs became more widespread, people were forced to look for alternatives to keep ahead of the crowd. Field Programmable Gate Arrays (FPGA) came into vogue for a brief period before Application Specific Integrated Circuits (ASIC) came onto the scene. ASICS can perform the Bitcoin hash at higher rates but with a much smaller energy requirement.

Bitcoin is similar to other currencies, in that the exchange rate between Bitcoin and other currencies fluctuates over time. This in turn impacts on the viability of Bitcoin mining; if the value of a Bitcoin is less than the cost of the energy required to generate it then there is a disincentive to continue mining. On the other hand, as the number of people mining Bitcoin increases, difficulty of mining follows suit, so the likelihood of discovering a valid block decreases. To overcome this, more powerful hardware is required to achieve the same success rate. However, since the cost of energy is a limiting factor, newer hardware will have to have a higher hash rate and a lower energy footprint. [11]

VI. What is Cloud and Why is it an Alternative

The key to the definition of cloud computing is "cloud" itself. Cloud is, by definition, a large group of interconnected computers. These computers can be personal computers or network servers and they can be public or private. For example, Google hosts a cloud that consists of both small PCs and large servers. Googles cloud is a private one which means it is accessible only by google users.

Cloud computing goes beyond a single company or enterprise. The applications and data served by the cloud are available to a broad group of users, across enterprises and across platforms. The access is via internet. Any authorized user can access these docs and apps from any computer over any Internet connection.

Cloud computing should not be confused with network computing where all the information are hosted on the company's single network and it can be accessed by members on that network only. Cloud is much bigger than that and it encompasses multiple companies, servers and networks.

In order to first think about implementing cloud technology with Bitcoin mining, it is essential to understand why a Cloud network based application is important. This can be explained by considering advantages of cloud computing, which are many but a few significant ones are listed as:

- Low-Cost Computers for Users: You do not need a high powered and highly priced computer to run cloud computing's web based applications. Because the application runs in cloud and not on the desktop PC, that PC does not need any processing power and Hard-disk space.
- Improvement in performance of computers: Because the desktop PC does not require to store and run tons of software applications, users will see better performance from their PC's. Put simply, computers on cloud network boot up faster and run faster because they have fewer programs and processes loaded in memory.
- Lower IT infrastructure cost: Instead of investing in larger numbers of more powerful servers, the staff of an IT company can use the computing power of the cloud to supplement or replace internal computing resources. These companies that have peak needs no longer have to purchase equipment to handle peaks in traffic.
- Lower software costs: Instead of purchasing separate software packages for each computer in the organization, only those employees actually using an application need access to that application in the cloud. Even if it costs the same to use similar desktop software, IT staffs are saved the cost of installing and maintaining those programs on every PC in the organization. Thus the costs of the software offered by cloud technology firms are much less than non-cloud firms.
- Fewer maintenance issues: Cloud computing substantially reduces both hardware and software maintenance cost for organizations. With less hardware in the form of fewer servers, the maintenance costs are immediately lowered. In the software front all applications are based on cloud servers, so maintenance practically zero.
- Cloud technology also offers unlimited storage capacity, increased data safety (as the data is not present directly on desktop it can be difficult for third party users to gain access), increased computing power and instant software updates (that is, when an application is updated by the owner or cloud service provider, this update is accessible to the users the next time they log in).

As a result of such attractive advantages pertaining to cloud services, Bitcoin mining can be made more efficient and cost-effective by exploiting various cloud technology services like:

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

VII. Bitcoin Cloud Implementation

Since the Bitcoin industry is very erratic in nature, it may not be feasible to own and operate costly ASICs and therefore the need to introduce cloud-technology to help reduce and recoup losses associated with high electricity consumption and maintenance cost for the users/customers. The term 'Cloud Mining' is coined for carrying out mining operations, associated with various cryptocurrencies like Bitcoins, on a cloud network.

The basic idea is that the miners can carry-out mining operations without requiring owning an ASIC but renting one. The renting of these machines provides easier exit opportunities to the miner in times when losses due to falling Bitcoin prices or increased difficulty in mining network are inevitable. This is an example of Infrastructure as a Service. The miners can also use platforms like amazon EC2 and Digital Ocean for mining, which is Platform as a Service. Finally the miners can simple rent/lease the hashing power of ASICs owned by large hardware companies that specialize in the development of integrated circuits (ICs).

To elaborate, there are three forms of cloud mining techniques miners can exploit for better profitability:

A. Hosted mining machines

This scheme can refer to hosted Bitcoin ASIC mining also where the miners, clients, can lease or rent ASICs. The clients are required to pay monthly rental rates for a large range of Bitcoin ASIC mining systems and can also rent a dedicated physical machine for their personal use. The advantages of such a scheme are obvious; for instance, clients can eliminate the electricity costs pertaining to running such machines at home as well as reduce carbon footprint. Further, miners need not worry about re-selling the machines at reasonable prices.

Many companies are working on their own hosted mining facilities, for example, KnC Miner, a Sweden based company is planning to introduce such a scheme in Stockholm and at the same time use renewable energy sources to power up the machines. A range of ASIC machines from 'Nano Fury NF2' with 3700 million/sec hash rate and 5 watts consumption to 'Hash Coins- Zeus v3' that has hash rate of 4.5 million/sec , electricity consumption of 3000 watts with USB COMM ports can be used under this scheme. The selection of the rigs depends on the client's budget and requirements.

B. Hosted platform mining

Under this scheme, a Client is required to rent virtual computers on which they can run their applications.

The Amazon EC2 platform:

The EC2 platform provides virtual services, also known as Compute Instances in the cloud quickly and inexpensively. The client is required to choose the instance type they want, selecting the templates which can be based on Windows or Linux and finally choosing the quantity of services (or virtual servers). This can be done by using the AWS management console or automate the entire process by an API using SDK in any programming language. After implementing the API code, client's instances will begin running and they will have full access and administrative control just like any other server. The EC2 provides a range of instance type designed for different use cases. These range from small and economical instances for low volume applications all the way up-to clustered computer systems for high performance computing workload and cloud based super-computing on demand. The amazon EC2 provides instances optimized for compute, memory, storage, GPU processing and also high performance ASICs. This enables clients to choose the right price and performance combination for whatever workloads to be run. It is also easy to resize the instance as the requirements of the clients change. For instance during time when the hashing rates and difficulty of the network are very high the user can adjust the instance to obtain high performance and vice-versa. The user will pay according to the degree of requirements of instances.

The important feature of Amazon EC2, it comes to determining the profitability of the platform, is the flexibility of the pricing options available to miners. With on-demand prices the clients pay for what they use that is if the instances are stopped the miners stop paying as well. Thereby, helping cut losses given the erratic nature of Bitcoin prices. The reserved instance price provides significant demand over the on-demand prices in return for low one-time payment. Spot instance prices lets the miners to name the prices they want to pay for instances using market based pricing and allows computing capacity at a significant discount compared to on demand pricing.

The spot instances prices are the most economical of the three models, whereby the miners can bid for computing time at a price they are willing to pay. When amazon has spare capacity, it will grant the computing power to the highest bidder and if the bid prices are too low then the mining system may never come online.

Further, EC2 mining provides a number of built-in security features to provide protection from Malware and Trojan attacks. The instances are located in a Virtual private cloud or VPC, which is a logically isolated network that the miners control. The VPC provides a number of network security tools, like Network ACLS and Security Groups, to determine who can access your instances.

A Security Group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. Clients can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

A Network access control list (ACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. Clients might set up network ACLs with rules similar to the security groups in order to add an additional layer of security to the VPC.[12][13][14]

DigitalOcean:

Another type of such service is provided by DigitalOcean. It is a provider of virtual private servers (VPS). These servers are not actual computers, but simulated computers – several of which run simultaneously on powerful server computers at once. This is a cost effective way for any business providing online hosting services whether it be virtual private servers or web hosts.

Usually, a group of virtual servers hosted on single (or across a network of) physical servers do not all need the CPU and network resources at once. Therefore, having several simulated computers contained within one physical computer is more efficient as one set of hardware can be active all the time, providing resources to all of the virtual machines it hosts. The whole business of virtual hosting is somewhat like fractional reserve banking in that it relies upon most of its users not requiring its resources at any particular moment.

C. Leasing hashing power

Under the scheme, the miners can rent Hashing power of multiple, highly powered ASICs machines owned by mining companies. The hashing rate depends on the plan chosen by miners. The plan must be selected while considering the profitability factor. The various service providers are:

- Cloud Hashing: A one year contract specifying the hashing power required is awarded to the clients under this service. Contracts can range from 30Gh/s to as much as 350Gh/s.
- Hash Rack: A single payment for an indefinite time is made by the clients (i.e., until the hardware breaks), a percentage of which can be reinvested to increase hashing power. Additionally, users can move 'hashpacks' between multiple rigs owned by them.
- Bit Miner: Offers collective mining on a rent sharing basis. For instance, the Ant Miner rig (6x180 GH/s) is divided into 10,000 shares, each of which is priced at $5.50. Several such rigs are rented at such competitive pricing.
- E-Pickaxe: Contracts vary from one year to indefinite length of time, payments for which are done using Bitcoins. However, the amount of GH per contract is not fixed because, as they put it "as we add more hardware, your contracts have access to that too, meaning as we grow and invest in more hardware, you benefit from this throughout the term of the contract".
- Bit of Glory: This firm offers 12-month contracts at 100 GH/sec, 500GH/sec and 1TH/sec.
- Cex.io: Clients using Cex.io can both mine as well as trade hashing speeds (GH/s). Profits are shared using the PPLNS (pay per last N shares) scheme and all hash-rates are guaranteed.
- Nimbus Mining: Nimbus Mining offers 12-month contracts of varying hashing powers, using 'off-the-shelf' hardware from various manufacturers, which can be chosen by the clients.
- eBay contracts: Several eBay users are currently offering mining contracts for a period of 24 hours for as little as £1 ($1.67). However, since these contracts are fulfilled on old USB Block Erupter rigs, the hashing power is limited. That said, this could set off a positive trend with powerful mining contracts being offered in the future.

VIII. Cloud Mining Efficiency Calculations

We have previously covered ways to calculate mining profitability for traditional mining methods. The difference is that the services offered are designed to work with the hardware parameters and not cloud-mining parameters.

Even so, we can still use these calculators by taking into account the costs involved. We had taken the example of Genesis block in determining profitability of hardware mining by multiplying the electricity charge ($ per KWh) by the power consumption of the unit and by a conversion factor of 0.744 (the ratio of seconds per month to joules of energy per KWh). But for cloud mining calculations we have to perform the opposite, mainly because the provider gives the miner an (effective) monthly running cost. Hence, we have to calculate the cost per kilowatt hour to feed into the mining calculator. This can be done by dividing the monthly running cost by the conversion factor (0.744) mentioned earlier. For example, if prospective/existing miners were to use these numbers into a Bitcoin mining calculator, they would enter '0' for the cost of hardware, shipping costs and miscellaneous costs, and enter '1' for power usage, and then enter the equivalent electricity cost into the electricity costs line.

However this type of calculation does not apply to all cloud mining service providers because some have a significantly different cost structure. Services provided by Hash Rack or Cex.io cloud mining companies, for example, would not be suitable for the calculations mentioned above.

IX. Limitations of Cloud

Engaging in any type of cryptocurrency mining can lead to risks but profits are possible if miners can make the right choices with regard to the factors mentioned earlier. While calculating profitability it is quite clear that some cloud mining services will be profitable for a few months, but as the difficulty level of the Bitcoin increases it is highly possible that miners start to make loses four to six months beyond.

Cloud Mining has been taking a beating with the precipitous drop in Bitcoin price over the past year. The profit margins have become thinner and thinner, and also non-existent for many miners and service providers. The value of less valuable altcoins has seen a corresponding tumble in value. On January 13, 2015 GHash.io reported that many as 30,000 miners are leaving the industry since BTC had entered the $300-and-below range.

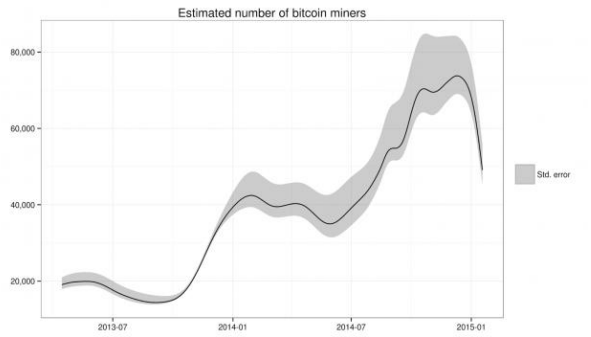

Fig. 3. Representation of the fall in Bitcoin miners [15]

The main reason for the mass exodus can be attributed to issues with paying off large loans for computer equipment, hosting services, rent and location leasing costs, all while keeping up with the latest in digital mining software and tech. These short-term costs can reach into the millions in dollars. As the price of Bitcoin has continued to drop, even the World's largest mining operations are unable to cover their costs at this time. In early 2015 CEX.IO, the second-largest Bitcoin mining pool extant, had temporarily suspended operations due to an inability to run their operation profitably. Another Bitcoin mining firm that has had to change with the times is GAW Miners. They moved into cloud mining in summer of 2014, and the company recently launched its virtual currency called Paycoin. Many customers who continue to mine using GAW's cloud-based "hashlets" have witnessed their operating fees starting to exceed the returns

from mining. If the market is having this much of an effect on the major player it is easy to estimate the effect on smaller service providers. Many have had to halt operations and payouts, including ZeusHash and PB Mining.

X. CONCLUSION

Since the start of the virtual currency revolution, the rate of evolution of mining techniques to maximize hashing rates (in turn maximizing profits) has been staggering. With mining machines and technologies becoming redundant at amazingly quick rates, stability has always been a question. It took only three years since the introduction of Bitcoins for miners to move from using their CPUs to buying mining specific ASIC machines. To make matters worse, the fluctuating values of the various cryptocurrencies make it impossible for any long term investment that does not involve considerable risks. The amount of computation required to validate transactions has been increasing exponentially because of two reasons – the complexity increases with each hash generated and the number of people entering the world of Bitcoin mining, which in turn increases the hash rate. Given the perilous scenario, where mining with privately owned ASICs and similar machines has the odds stacked against it when it comes to profitability, cloud mining by leasing machines seems to be the way forward, as it offers greater chances of profit and easier exit options with a very low initial investment.

The flipside is that even for many of the cloud mining providers, this initial short term investment to buy large and powerful mining machines, security features, space, air conditioning for the systems and electricity to power them is way too high, as can be seen from the temporary suspension of operations of key players such as cex.io. With stringent government regulations, and a general negative outlook on cryptocurrencies, sudden drops and rises in the value of Bitcoins is bound to happen time and again and miners need to be braced for it. What one needs to keep in mind is that, such sudden drops notwithstanding, value of Bitcoins, and cryptocurrencies in general would rise proportionally to the increase in hashing difficulty.

For cloud mining to be successful, miners need to move from private mining techniques and adopt cloud mining on a larger scale, which would only then justify the initial expenses of these cloud service providers. A dangerous scenario that may arise when this does not happen is that several of these providers would face losses and ultimately quit, leaving only few giants such as Amazon or Digital Ocean in business, who would then gain complete dominance over the mining network, leading to monopoly. Not only is this unhealthy to the mining network, it is against its fundamental nature that the system is decentralized and provides equal opportunities to all miners.

This paper provided an in depth view of types of cryptocurrencies currently in operation, the types of mining algorithms and the history of machines used for mining process, which led us to the next logical step of cloud based mining. But of course, this is definitely not the final solution. As complexity and competition increases, faster and more efficient machines are bound to be designed. However, at present, cloud mining presents the most viable route to maximizing profits.

REFERENCES

[1] Morgan E. Peck - The Bitcoin Arms Race is on! Spectrum, IEEE, vol.50 (2013), Issue: 6, pp. 11-13.

[2] Allied Control – Analysis of Large-Scale Bitcoin Mining Operations (White Paper), URL: http://www.allied-control.com/publications/Analysis_of_Large-Scale_Bitcoin_Mining_Operations.pdf.

[3] Brito, J. & Castillo, A. (2013). Bitcoin: A Primer for Policymakers.

[4] S. Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System," URL: https://bitcoin.org/bitcoin.pdf, 2008.

[5] The cryptographic hash function SHA-256, URL: http://www.researchgate.net/publictopics.PublicPostFileLoader.html?id=534b393ad3df3e04508b45ad&key=50463534b393ab994e.

[6] Evans-Pughe, C.; Novikov, A.; Vitaliev, V.-"To bit or not to bit?". Engineering & Technology, vol. 9 (2014), Issue: 4, pp. 82-85

[7] Hurlburt, G. F; Bojanova I. - "Bitcoin: Benefit or Curse". IT Professional, vol. 16(2014), Issue: 3, pp. 10-15.

[8] Taylor, M. B - "Bitcoin and the age of Bespoke Silicon". Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2013 International Conference, 2013, pp. 1-10

[9] Mining Hardware Comparison, URL:https://en.Bitcoin.it/wiki/Mining_hardware_comparison

[10] Bitcoin Difficulty. URL: https://Bitcoinwisdom.com/Bitcoin/difficulty

[11] O'Dwyer, K. J.; Malone, D. - "Bitcoin Mining and its energy footprint". Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET, pp. 280-285

[12] Amazon EC2. URL: http://aws.amazon.com/ec2/

[13] Amazon Elastic Compute Cloud. URL: http://en.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud

[14] Amazon EC2 Security Groups for Linux Instances. URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

[15] January 18th 2015 Network Statistics. URL: http://organofcorti.blogspot.com.au/2015/01/january-18th-2015-network-statistics.html