Optimizing Bitcoin Generation and the Feasibility of Profitability

Michael Sprague, *Undergrad at UC Santa Barbara*

Abstract—**Bitcoin is a decentralized and digitized form of currency that has recently gained traction. Although it is not backed by a physical resource such as gold or silver, it is still possible to ”mine” Bitcoin by solving computational puzzles. The goal of this paper is to provide insight into the mining process, propose various hardware solutions to maximize output, and analyze the results of different mining techniques to determine the cost-effectiveness of harvesting Bitcoin.**

Keywords—Bitcoin, SHA-2, Blocks, Mining.

I. Introduction

BITCOIN is a new subset in research for Computer Science. The idea originated from Satoshi Nakamoto's self-published paper in 2008 entitled *Bitcoin: A Peer-to-Peer Electronic Cash System* [1]. His paper proposed a decentralized and digitized form of currency, Bitcoin, which is not backed by a physical resource, such as gold or silver. As a result, no single entity (a central bank, government, or corporation) can manipulate the currency through printing new physical denominations. In addition, Bitcoin allows for a certain amount of anonymity since transactions are linked to identifiers, not to legal names. Recent research has dissected the implementation of Bitcoin to shed light on its potential pitfalls. Economic approaches argue that the focus of Bitcoin's decentralized nature is irrelevant, since any currency controlling government can purchase advanced equipment to mine Bitcoin. However, research in Computer Science has focused on potential security exploits of Bitcoin. For example, anonymity can be comprised via traversal of transaction nodes in the network. In addition, many papers focus on more effective forms of mining and securing Bitcoin, since the fear of SHA-based computational puzzles become trivialized once quantum computing advances.

With the recent public exposure of Bitcoin, the massive amounts of investments coming from Europe (Cyprus), and the large amount of Bitcoin miners, the value of Bitcoin has increased over one hundred fold, creating another gold rush. Many papers have dug into the implications of a cap to mining Bitcoin, but not many have touched upon the financial opportunity of mining Bitcoin itself. Is this because it is unreasonable to assume that there is profit to be made in mining Bitcoin? If that is the case, then why are so many people rushing to mine Bitcoin? The purpose of my research is to propose methods to shed light on the current state of Bitcoin mining and resolve whether or not mining Bitcoin can be valuable. Is this a true gold rush or simply a colossal waste of time and energy?

II. Background

SATOSHI Nakamoto, whose true identity is unknown, invented Bitcoin in a self-published paper in October 2008. The decentralized nature and speed of transactions of Bitcoin has lead to a massive gain in popularity [2], thus creating value for this digital currency. Since the inception of Bitcoin, the trading price has varied from sub one dollar to over 200 dollars in only a few years. As it currently stands, one Bitcoin is approximately worth 120 dollars.

A. Mining

Bitcoin are created using ”Bitcoin miners” that solve computational puzzles known as blocks [3]. By solving a block, the miner has both verified a transaction's validity and generated multiple Bitcoin for itself. The number of Bitcoin rewarded to the miner depends on the total number of solved blocks in existence. The initial reward was 50 Bitcoin, but has since halved to 25 and will continue to half after the completion of every 210,000 blocks until 21 million Bitcoin are in existence, in which case no more coins can be mined [4]. There are currently approximately 11 million coins in circulation.

B. The Bitcoin Wallet

Bitcoin are associated pseudo anonymously with an address and a private key that are generated and stored with a user's wallet. The address acts similar to a physical building address– it allows a source or destination for Bitcoin transfer. The private key acts as the user's personal signature and proof to guarantee each transaction's success. While a wallet is not truly anonymous (it has a public identifier associated with it), the personal identity of the user is not linked to the address, private key, or wallet.

C. Transactions

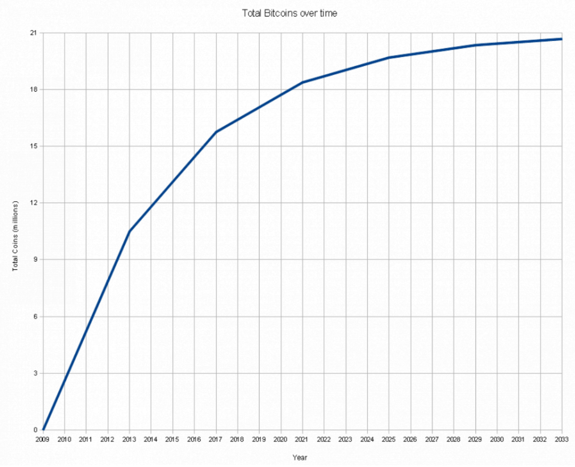
Satoshi Nakamoto cleverly invented a way of joining Bitcoin transactions and mining. Two addresses that wish to exchange Bitcoin must find a third party to verify the transaction. A transfer request creates a ”block” which contains the transfer information along with a computational puzzle that must be solved by a third party. Upon solving the puzzle, the transaction is verified, added to block chain, and the solver is rewarded with newly minted Bitcoin which are considered ”mined”. In addition, the two exchanging addresses may provide a Bitcoin commission as incentive to motivate other parties to verify the transaction more quickly. Upon success, the transaction is added to the ledger, or block chain, that contains a history of all transaction between different addresses.

D. Generating Blocks

Mining Bitcoin involves the process of solving a computational puzzle to create a block which both verifies a transaction and generates Bitcoin. While it is almost exclusively referred to as a puzzle, in reality the process of generating a block is more akin to playing the lottery. Each client attempting to generate a block randomly picks a number, computes the SHA-2 of that number, then checks the result against a valid range. If the result falls within that range, the randomly picked number is considered a solution to the puzzle, and a block is created rewarding the party with mined Bitcoin and commission, if offered. Thus, an efficient Bitcoin mining machine will generate and check as many random numbers as possible for maximum potential Bitcoin generation.

E. Minted Bitcoin

The number of Bitcoin minted per each successful block decreases over time and the difficulty of creating the block increases. This emulates the behavior of a physical resource, such as gold or silver, that depletes over time and eventually is completely eradicated from mining. At the time of writing this paper, 25 Bitcoin are rewarded for a successful block, however that number will half every 210,000 blocks. Theoretically, this should happen once every four years until a maximum of 21 million Bitcoin are in circulation, which is estimated to occur in 2140 [4].



”Total estimated Bitcoin over time, assuming a perfect 10-minute interval.”[4]

Presently, there are just over 11 million. This event, although gradual, would have many implications that are out of the scope for this paper (deflation, for example).

III. Problem

WITH the ever decreasing number of Bitcoin minted,2,016 can mining be profitable? If so, what is the optimal hardware and software needed to efficiently mine Bitcoin, and how long will mining continue to be profitable? I will explore various ways of generating Bitcoin and propose methods to quantify the cost of the equipment (including expenses for electricity, but assuming the cost of Internet access is negligible) and compare it to the exchange value of Bitcoin to USD.

IV. Mining Techniques

SNICE Bitcoin is mined by generating and guessing SHA-2s to solve blocks, the most efficient machine would generate as many SHA-2 hashes as possible (known as the ”hash rate”) while using as little energy as possible.

A. CPU Mining

Because a CPU, Central Processing Unit, is optimized for performing complicated, parallel tasks, computing SHA-2 hashes on a CPU is more slow and inefficient than any other alternative. On average, each CPU core can perform no more than 4 instructions per clock cycle. While this is effective for many tasks, Bitcoin mining is not one of them. The average hash rate of a CPU is around 3 million hashes per second, or 3 Mhash per second, which is extremely slow compared to other hardware. In fact, CPU mining is no longer officially supported by the Bitcoin mining client! [4]

B. GPU Mining

A GPU, Graphics Processing Unit or video card, is a specialized piece of hardware that is in charge of computing graphics operations and displaying visuals on a monitor. Due to the need to perform numerous amounts of mathematical equations per second to render graphics, GPUs are optimized to operate with a very high clock rate. A modern graphics card executes around 3200 instructions per clock cycle; 800 times more than a CPU! A GPU can compute between a few hundred to a few thousand Mhash per second, depending on the graphics card. [4]

C. FPGA Mining

An FPGA, Field Programmable Gate Array, is a small, efficient piece of hardware used primarily for integration with circuits and specialized computing. Unlike a CPU or GPU, it does not run within a computer–instead it is standalone and programmable, meaning that it performs a specific task constructed with software by the user of the device. When configured for mining Bitcoin, FPGAs perform akin to a GPU, typically producing between 100 Mhash per second and 1 GHash per second. However, an FPGA is more energy efficient than a GPU because it runs standalone. [4]

D. ASIC Mining

The most efficient hardware for mining Bitcoin is known as an ASIC, or Application-Specific Integrated Circuit. Each type of ASIC is specifically designed and manufactured for a corresponding application. There currently exist less than twenty major types of ASICs used for mining Bitcoin and are in very limited supply. Unlike an FPGA, the hardware of a Bitcoin-mining ASIC is specifically designed and optimized for mining Bitcoin, meaning that there is no theoretical limit to the number of hashes per second that can be computed with ASIC hardware. Low-end ASIC miners produce around 300 Mhash per second, while high-end miners can generate anywhere from 60 GHash to 1.5 THash (one trillion hashes) per second. The performance of an ASIC miner is incredibly high and will likely render FPGAs and GPUs useless for Bitcoin mining in the near future as mining Bitcoin becomes more difficulty. However, the production of Bitcoin-mining ASICs begun in early 2013 and quantities are extremely limited to consumers at this time. [4]

E. Pooling

While the above techniques discuss specific hardware used by a single client to mine Bitcoin, there exists a distributed method to collect Bitcoin. The only way to mine a Bitcoin is through block generation with SHA-2, however since block generation is akin to buying lottery tickets, the rewarded Bitcoin collected can be far between. To reduce the amount of time it takes to receive a Bitcoin payout, software engineers have created a distributed mining technique called pooled mining. Pooled mining allows multiple clients to group their efforts together towards the generation of a block, then split the reward amongst themselves according to the processing power contributed. Each client attempts to solve a block of an easier difficulty which is a superset of the original block (the range of ”winning tickets” is larger). If the easy block is solved, the client gets a point for work, and if the original block is solved, the Bitcoin are successfully mined and distributed to the clients depending on how many points they currently have. This technique allows for a smaller, uniform payout of Bitcoin, instead of large payouts that come infrequently. Theoretically, the client will receive a similar payout to solitary mining, but in smaller, more frequent increments [4].

V. Probabilities and Difficulty

THE ever decreasing number of minted Bitcoin and ever increasing difficulty in mining Bitcoin imply that mining will become more costly in the future. In order to successfully solve a block, the client must generate a SHA-2 that resides within the current target. As more blocks are generated, the difficulty of the problem increases and the current target's value decreases.

A. Current Target

The current target is a 256-bit number known by all Bitcoin clients. In order to solve a block, the client must guess a value, perform a SHA-256 hash function on that value, then check if the resulting value is less than the current target. The goal of the current target is to keep 2,016 blocks generated every two weeks, or one block every ten minutes. Since new Bitcoin miners are being introduced each day, the current target is lowered to force approximately 2,016 blocks generated every two weeks, else all 21 million Bitcoin could be mined extremely quickly with new hardware. After every 2,016 blocks generated, the current target is modified by the percentage difference in between the amount of time it took to generate those blocks and the desired time (2 weeks)[4]:

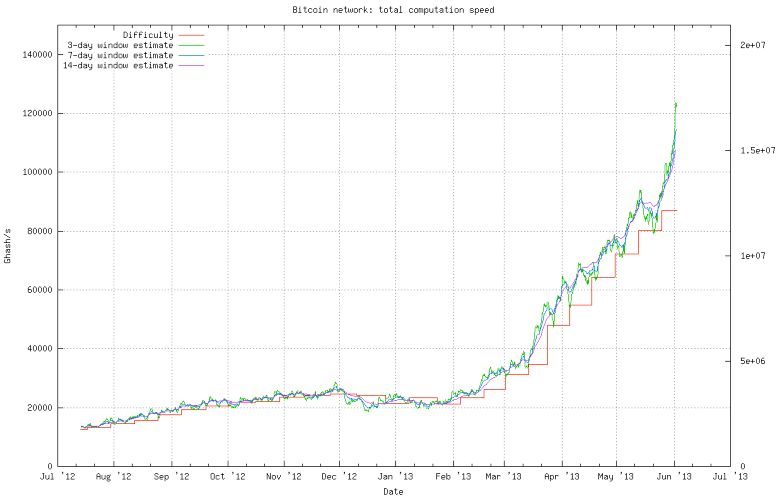
$$new\ target = current\ target \times \frac{time\ since\ last\ 2{,}016\ blocks}{2\ weeks}$$

B. Current Difficulty

The current difficulty is a metric used to approximate the time to mine a Bitcoin based on a hash rate. It is defined as:

$$difficulty = \frac{maximum\ target}{current\ target}$$

Since the current target calculated is based on the speed of the blocks generated, there is a direct correlation between the total hash rate of all miners and difficulty. The difficulty and hash rate are directly proportional and can be charted over time:



Increase in difficulty and total hash rate over time [4]

As expected, the rise in popularity of Bitcoin increased the total hash rate (the sum of the hash rate of each miner) and thus, increased the difficulty.

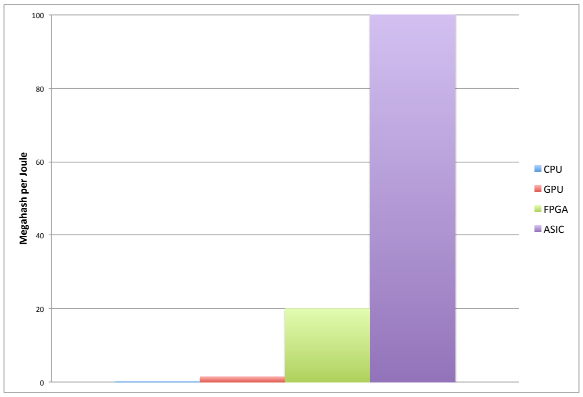
C. Expectancy Estimation

The following formula uses the current difficulty to estimate the expected time to mine Bitcoin by solving a block:

$$(I) \quad time = \frac{difficulty \times 2^{32}}{hash\ rate}$$

VI. Power Consumption Efficiency

EFFICIENCY while mining Bitcoin is one of the most important factors for profitability. If the cost of mining a single Bitcoin exceeds the value of a Bitcoin, then there is no point to mining. Fortunately, the fastest hash rates come with the most simple and fast hardware that use the least amount of power. The following chart shows the amount of energy (in joules) needed to compute one thousand hashes (Mhash per Joule).



Megahash generate per joule for each type of hardware (The data has been averaged from the Bitcoin Wiki [4])

As expected, the most efficient method for mining Bitcoin is using ASICs (100 Mhash/joule). In addition, an FPGA is approximately twenty times more efficient than a GPU.

VII. Methods

DIFFERENT specific hardware options for Bitcoin mining will be explored and the number of mined Bitcoin will be recorded, along with the total cost of the equipment and upkeep. The most efficient solution will be chosen and extrapolated to estimate the Bitcoin generation rate in the future. There will be four machines: one low end (CPU mining), one high end (expensive GPU), one FPGA, and one mining specific machine (ASIC). Each machine will run independently in a pool for a fixed amount of time (preferably a couple months) and the number of Bitcoin will be recorded and compared. These empirical results are extremely important due to the unknown nature of the increase in difficulty in the future. However, these calculations can be performed theoretically using the current difficulty.

VIII. Theoretical Results

FOR the following theoretical experiments, we assume a current difficulty of 12153411.709776 (as of June 1st, 2013) and use the estimated hash rate for each piece of hardware to calculate the time to solve a block. The caveat to this experiment is that it does not account for a change in difficulty over time.

A. CPU

An Intel Core i7 620M runs at a clock speed of 2.66Ghz. Using data from the Bitcoin Wiki [4], we observe a hash rate of 6.3 Mhash per second and power consumption of 0.18 Mhash per joule. Using formula (I), we can estimate that this machine would solve a block every 95,897 days, or 262.7 years.

B. GPU

An AMD Radeon 6970 runs at 1375MHz. On average, this card outputs 397 Mhash per second and 1.89 Mhash per joule. It is ten times more efficient and 63 times faster at solving blocks than the CPU used above. Using formula (I), this video card would solve a block every 1,521 days, or 4.17 years.

C. FPGA

A specialized FPGA, BitForce SHA256 Single, computes 832 MHash per second and 10.4 MHash per joule. This is approximately ten times more efficient than the GPU and one hundred times more efficient than the CPU. This FPGA solves a block approximately every 726 days, or 2 years. *Note: this is not an average FPGA.*

D. ASIC

ASIC Bitcoin miners are currently difficult to obtain. For this experiment, we will assume that we are using an Avalon ASIC 1 which produces 66,300 Mhash per second and 52.34 Mhash per joule. **On average, this machine solves one block every 219 hours, or 9.1 days.**

IX. Analysis

THE calculations have been compressed and populated into the table below. Each entry assumes the USD to Bitcoin rate is $120. kW/BTC denotes the total number of kilowatts used to mine a single Bitcoin, Profit Per Bitcoin is calculated by the following equation:

$$profit = btceUSD - \frac{kW}{BTC} \times \frac{price}{kWH} \times hours$$

Where price per kWH is the average cost of electricity in the United States at the time of writing, 12.8 cents [5].

Hardware	kW/BTC	Profit Per Bitcoin	Profit Per Month
Intel i7	3222	-$292	-$2.29
Radeon	365	$73	$36.13
BitForce	55.8	$113	$116.59
Avalon	5.4	$119	$9832

X. Conclusion

We have seen the mathematical functions that model the difficulty and provide estimations for the process of Bitcoin mining. We can expect to see physical results that are accurate to our estimations. If the goal is to optimize Mhash/dollar, then we should purchase an ASIC miner. This would generate about 2.64 Bitcoin per day, decreasing each time the current target is decreased. At the time of writing this paper, the purchase of an efficient ASIC is extremely profitable. An initial investment of $1,300 that produces 66,300 Mhash per second would turn a profit after four days and generate $9,832 per month including electricity expenses. However, the purchase of such a device will no longer be profitable if *any* of the following conditions are met.

1. The replacement time of the device becomes less than the time required to turn a profit.

2. The price of a Bitcoin becomes less than the cost of mining a Bitcoin:

$$cost = \frac{kW}{BTC} \times \frac{price}{kWH} \times \frac{difficulty \times 2^{32}}{hash\ rate}$$

Presently, this machine is profitable at an exchange rate of five us dollars per Bitcoin, making $354.95 per month after the first three and a half months cover the fixed cost of the device. However, there are two main unknowns about the future of Bitcoin mining. First, we do not know how many miners will enter the market in the future. If the total number of MHash per second increases drastically, the difficulty will also increase drastically resulting in a much lower rate of generation of Bitcoin. Second, the value of Bitcoin is purely speculative. It is possible that Bitcoin is simply a bubble that will pop in the coming months and the value of a Bitcoin will decrease to near zero. In addition, the output of block generation will halve in three and a half years, however if the above two conditions hold in our favor, we will have made $412,944 in profit and the mean time.

REFERENCES

[1] Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System.* Available online at *http://bitcoin.org/bitcoin.pdf*. 2008.

[2] Moshe Babaioff , Shahar Dobzinski , Sigal Oren , Aviv Zohar, *On Bitcoin and Red Balloons*. Proceedings of the 13th ACM Conference on Electronic Commerce. June 04-08, 2012.

[3] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun, *Bitter to Better - How to Make Bitcoin a Better Currency*. Financial Cryptography, vol. 7397 of Lecture Notes in Computer Science, pp. 399-414. 2012.

[4] BITCOIN. *The Bitcoin Wiki.* Available online at *https://bitcoin.it*.

[5] Bureau of Labor Statistics. *Average Energy Prices for the U.S. and Selected Metropolitan Areas.* Available online at *http://www.bls.gov/ro5/ro5econ1.htm*.