Bitcoin Mining and its Energy Footprint

Karl J. O'Dwyer[†] and David Malone[*]

Hamilton Institute
National University of Ireland Maynooth

E-mail: [†]karl.a.odwyer@nuim.ie [*]david.malone@nuim.ie

Abstract — **Bitcoin is a digital cryptocurrency that has generated considerable public interest, including both booms in value and busts of exchanges dealing in Bitcoins. One of the fundamental concepts of Bitcoin is that work, called mining, must be done in checking all monetary transactions, which in turn creates Bitcoins as a reward. In this paper we look at the energy consumption of Bitcoin mining. We consider if and when Bitcoin mining has been profitable compared to the energy cost of performing the mining, and conclude that specialist hardware is usually required to make Bitcoin mining profitable. We also show that the power currently used for Bitcoin mining is comparable to Ireland's electricity consumption.**

Keywords — **Bitcoin**

I Introduction

Bitcoin is a peer-to-peer cryptocurrency mainly used for monetary transactions on the Internet [1] and is designed to be similar to fiat money and commodities. Bitcoins are intrinsically valueless, their worth is decided by those trading in them. At the time of writing, 1 Bitcoin (฿) is worth approximately 378.7 Euro(€). Bitcoin has generated a huge amount of interest in the media lately and has sparked a wave of copy-cat-currencies (Litecoin, Gaelcoin, etc.) and even a fully working parody currency (dogecoin). It has also generated interest in academic circles due to issues it creates in user privacy e.g. [2], as well as attempts to gain insights into is behind transactions e.g. [3] and attempts to better understand its implications as a payment system e.g. [4].

Bitcoin is based on a peer-to-peer network within the Internet. The members of the peer-to-peer network effectively maintain a ledger of Bitcoin transactions which have been accepted by the network. In this ledger, Bitcoins are owned by *Bitcoin addresses*, which are public keys from a keypair. In order to assign Bitcoins, or some fraction thereof, to a new owner, the current owner must sign the transaction with the private key of the keypair using an ECDSA scheme. Before a transaction is accepted by the network, the transaction is checked for validity, including the presence of these signatures.

Bitcoins are not issued or governed by a central authority but, instead are created in a process called *mining*. Mining is one of the key concepts behind the Bitcoin protocol, in which valid transactions are collected into *blocks* and are added to the ledger by linking it to the previously accepted blocks. The network forms a common view, called the *blockchain*, of which transactions have taken place, preventing users from reusing Bitcoins and attempting to spend them more than once.

To add a block to the blockchain, a signature must be found linking the transactions in the block to the previous blocks. This requires finding a *nonce* value which satisfies a particular equation involving the SHA256 cryptographic hash function. This is a computationally expensive task; however, a member of the peer-to-peer network who finds a suitable value is rewarded by being able to assign newly mined Bitcoins to an address of their choosing.

In this paper we consider the energy cost of Bitcoin mining. Solving of the computational problem requires energy. We consider how this energy can be calculated and the impact of using different types of hardware for this computation. Using historical information from the Bitcoin network and

Bitcoin exchanges, we compare the monetary cost of the energy to the reward for calculating a Bitcoin block. We also consider the likely power consumption of the whole Bitcoin mining operation, and show that it is comparable to Ireland's average electricity consumption.

II Bitcoin Mining

As we mentioned, 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, based on the ideas of Hashcash[5]. In this scheme, there is a current target value T, which is periodically recalculated by the network (see Section II.a)). The miner's aim is to find a nonce value so that

$$H(B.N) < T \tag{1}$$

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

$$H(S) := \text{SHA256}(\text{SHA256}(S)).$$

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*.

II.a) Difficulty

The rate at which Bitcoins can be discovered can be controlled by the Bitcoin Network's choice of the value of the target, T, in eq.1. However, the target depends on the current number and speed of miners in the Bitcoin network, and is normally quoted in terms of the *difficulty*, D. The relationship between the difficulty and the target T is

$$D = \frac{T_{\max}}{T}$$

where the largest possible value of the target $T_{\max}$ is $(2^{16}-1)2^{208} \approx 2^{224}$.

The hash function H for Bitcoin has been chosen so that it behaves approximately as a uniformly random value between 0 and $2^{256}-1$. Thus, for any given nonce value, the probability of it satisfying eq.1 is

$$p = \frac{T}{2^{256}} = \frac{T_{\max}}{D2^{256}} \approx \frac{1}{D2^{32}}.$$

Each nonce value tested should behave like an independent trial, so the number of trials until a block is successfully completed will be geometrically distributed, therefore the the expected number of hashes to find a block is $D2^{32}$. If we have a system calculating hashes at a rate R, the expected time to find a block is

$$\mathbb{E}[t] = \frac{1}{p} \approx \frac{D2^{32}}{R}. \tag{2}$$

For example, if you can calculate a Bitcoin hash 1 million times a second, and the difficulty is $4,250,217,920$[1], then $\mathbb{E}[t] \approx 1.8 \times 10^{13}$s.

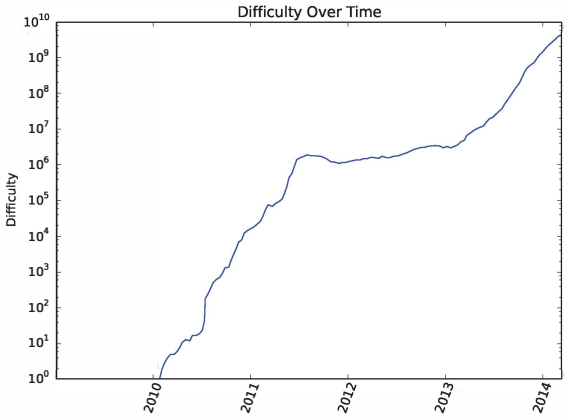

Fig. 1: The change of the difficulty to generate a Bitcoin over time, based on aggregated statistics [6].

II.b) Change in Difficulty

The difficulty, D, is recalculated every 2016 blocks, with the aim of keeping the average time to discover a new block near 10 minutes. At this ideal speed, 2016 blocks will be discovered every two weeks. To calculate the new difficulty, the length of time that it took to calculate the the last 2016 blocks is used to estimate the hash rate of the entire Bitcoin network. The new difficulty is selected so that if the same average hash rate is maintained, it will take two weeks to calculate the next 2016 blocks. If the resulting difficulty is more than four times harder (or four times easier) than the current difficulty, then the result is capped to four times harder (or easier). Restrictions on the range of acceptable difficulties/targets are also applied. The historical values of difficulty to date are shown in Figure 1. The increasing trend in difficulty has been caused by an increase in the resources dedicated to calculating hashes in the Bitcoin network.

II.c) Change in Reward

There are two sources of reward for calculating a new block. First, the block is formed from Bitcoin transactions, and a transaction may choose to include a transaction fee, to be paid to whoever finds a block containing this transaction. Sec-

[1]Current as of mid March 2014.

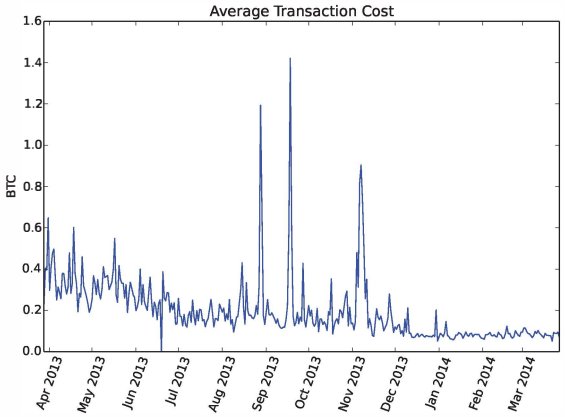

Fig. 2: The average transaction fee per block per day. Data derived from `http://blockchain.info/charts`.

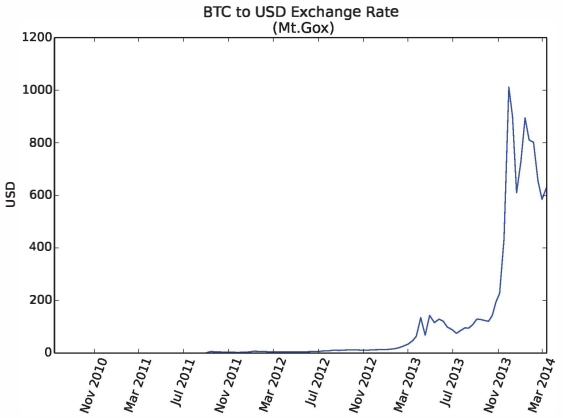

Fig. 3: The exchange rate between Bitcoin and Dollars, based on aggregate statistics [6].

ond, a standard reward is provided depending on how many blocks have been successfully calculated. This reward started at ฿50 per block and is halved every 210,000 blocks. As of mid-March 2014, the reward is ฿25. The reward will eventually reach ฿0; after such time it is imagined that the network of miners will continue mining but will do so in order to gain processing fees. This means that there is a limit on the number of Bitcoins which will be mined, but each Bitcoin is divisible up to 8 decimal places.

The mean value of the transaction fee over a day is plotted for a range of days in Figure 2. As we can see the current standard reward, ฿25, is considerably larger than the current or historical average transaction fees. This may change in the future, as the standard reward continues to halve.

III Hardware Arms Race

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 $\mathcal{E} = R/P$ (Mhash/J) which serves as a helpful statistic to compare hardware. Statistics are shown for a selection of hardware in Table 1.

Initially mining took place on normal[2] 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 or 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. The evolution of hardware for Bitcoin mining is described in detail in [7].

IV Energy Cost/Reward Trade Off

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 generated it then there is a disincentive to continue mining. The exchange rate to US dollars is shown in Figure 3.

On the other hand, as the number of people mining Bitcoin increases and the 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.

Thus, there is a trade off between two time varying factors: first, the energy cost of discovering a block,

$$C_e = \mathbb{E}[t]PU \approx \frac{D2^{32}PU}{R} = \frac{D2^{32}U}{\mathcal{E}}$$

where U is the unit cost for a Joule of energy; second is the cash reward for discovering the block, which is simply the reward for the block, in ฿,

[2]Where 'normal' is defined as a general purpose computer, such as an IBM PC type architecture with an x86 CPU.

Name	Type	Hash Rate R (Mhash/s)	Power Use P (W)	Energy Efficiency $\mathcal{E}$ (Mhash/J)	Cost ($)	Reference
Core i7 950	CPU	18.9	150	0.126	350	[8, 9]
Atom N450	CPU	1.6	6.5	0.31	169	[10, 9]
Sony Playstation 3	CELL	21.0	60	0.35	296	[11, 9]
ATI 4850	GPU	101.0	110	0.918	45	[12, 9]
ATI 5770	GPU	214.5	108	1.95	80	[13, 9]
Digilent Nexys 2 500K	FPGA	5.0	5	1	189	[14, 9]
Monarch BPU 600 C	ASIC	600000.0	350	1714	2196	[15, 9]
Block Erupter Sapphire	ASIC	333.0	2.55	130	34.99	[16, 9]

Table 1: Examples of Bitcoin-mining devices.

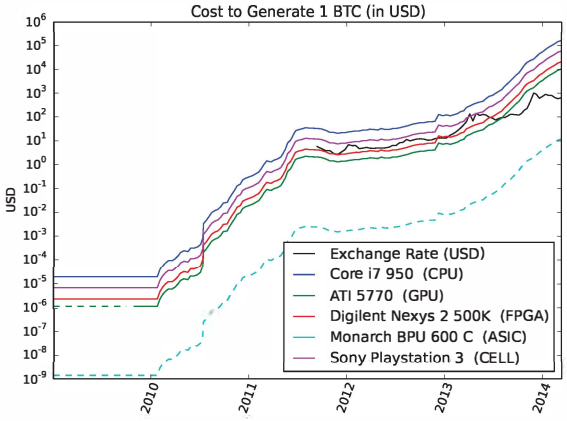

Fig. 4: The Cost of Generating a Bitcoin and the value of the resulting reward.

times the current exchange rate for a Bitcoin. Alternatively, we may normalise this per Bitcoin. Figure 4 shows the energy cost and the value for generating a Bitcoin for various hardware from Table 1. We use a dashed line for hardware before its release.

To allow easy comparison with the Bitcoin exchange rate, we use a cost of 0.10 US dollars per kWh. This is the lowest cost of electricity in Eurostat's 2013 statistics[17]; for Industrial rates in Finland. As typical consumer prices are twice this or more, this should provide a lower bound for the energy cost of mining Bitcoins in Europe. When calculating the value of each block, we have used the standard reward and not included transaction fees, as we have seen that the transaction fees are uncertain and currently a small fraction of the total reward.

For the period for which exchange rate data is available, we see that it has never been profitable to use a generic Core i7 CPU, and it appears that it may only have been briefly been profitable to use a Playstation 3. Using FPGAs or GPUs appears to have been close to profitable until mid-2013, when the increase in difficulty outpaced the increase in Bitcoin value. The yet-to-be-available ASIC hardware could be profitable, though the gap is closing.

V Network Power Usage

As we know that the Bitcoin network aims for an aggregate block discovery rate of one every 10 minutes, we can use eq.2 to estimate the hash rate of the entire network if we know the difficulty:

$$R_{\text{net}} \approx \frac{D2^{32}}{600s}.$$

Combining this with the efficiency $\mathcal{E}$ for different hardware, we can estimate the network's power usage as $P_{\text{net}} = R_{\text{net}}/\mathcal{E}$. For commodity hardware (CPUs/GPUs), efficiency values above 2 Mhash/J are unlikely[9]. For FPGAs, values around ten times this are possible. For ASICs values of 100–1000 times are possible.

Figure 5 shows conservative estimates for the total power used for Bitcoin mining, assuming that it consists of either efficient commodity hardware ($\mathcal{E} = 2$ Mhash/J) or efficient specialist hardware ($\mathcal{E} = 2000$ Mhash/J). The actual network will be a mix of hardware of types at different levels of efficiency, so we expect that the actual efficiency will be between the two. This suggests that the total power used for Bitcoin mining is around 0.1–10GW. Average Irish electrical energy demand and production is estimated at around 3GW [18, 19], so it is plausible that the energy used by Bitcoin mining is comparable to Irish national energy consumption.

VI Conclusion

In this paper, we have described aspects of Bitcoin relevant to Bitcoin mining and its energy consumption. Even though the value of Bitcoin is decided by those who trade in them, it is also related in some way to the value of electricity. We have seen that the cost of Bitcoin mining on commodity hardware now exceeds the value of the rewards. Thus, the competition created in mining for Bitcoin has lead to a situation where in order to be financially viable the hardware has had to become faster and more energy efficient.

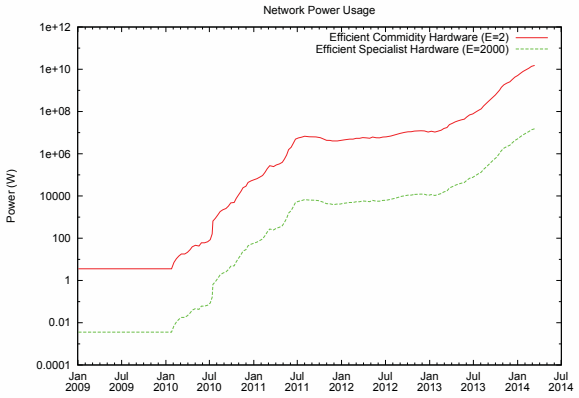

Fig. 5: Estimated Power Consumption of the Bitcoin Mining Network.

In this paper we looked at the energy issues around Bitcoin mining and its profitability. We also estimated under reasonable, reasonable assumptions, that currently the entire Bitcoin mining network is on par with Ireland for electricity consumption.

Acknowledgements

This research was supported by HEA PRTLI Cycle 5 TGI.

References

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. `http://fastbull.dl.sourceforge.net/project/bitcoin/Design\%20Paper/bitcoin.pdf/bitcoin.pdf`.

[2] Elli Androulaki, GhassanO. Karame, Marc Roeschlin, Tobias Scherer, and Srdjan Capkun. Evaluating user privacy in bitcoin. In Ahmad-Reza Sadeghi, editor, *Financial Cryptography and Data Security*, volume 7859 of *Lecture Notes in Computer Science*, pages 34–51. Springer Berlin Heidelberg, 2013.

[3] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. A fistful of bitcoins: Characterizing payments among men with no names. In *Proceedings of the 2013 Conference on Internet Measurement Conference*, IMC '13, pages 127–140, New York, NY, USA, 2013. ACM.

[4] Ghassan O. Karame, Elli Androulaki, and Srdjan Capkun. Double-spending fast payments in bitcoin. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 906–917, New York, NY, USA, 2012. ACM.

[5] Adam Back et al. Hashcash-a denial of service counter-measure. `ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf`, 2002.

[6] Stephen Gornick and Adrian. Bitcoin difficulty adjustments. `https://docs.google.com/spreadsheet/ccc?key=0AiFMBvXvL2dtdEZkR2J4eU5rS3B4ei1iUmJxSWNlQ0E#gid=0`, 2014. [Online; accessed 27-March-2014].

[7] Michael Bedford Taylor. Bitcoin and the age of bespoke silicon. In *Proceedings of the 2013 International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, page 16. IEEE Press, 2013.

[8] Amazon. Intel Core i7-950 3.06 GHz 8 MB cache socket LGA1366 processor. `http://www.amazon.com/Intel-i7-950-Socket-LGA1366-Processor/dp/B002A6G3V2`, 2014. [Online; accessed 19-March-2014].

[9] bitcoin.it. Mining hardware comparison. `https://en.bitcoin.it/wiki/Mining_hardware_comparison`, 2014. [Online; accessed 19-March-2014].

[10] Amazon. Intel Atom N450 processor. `http://www.amazon.com/CPU-Central-Processing-1-66GHz-FCBGA559/dp/B00HKIFV5O/`, 2014. [Online; accessed 19-March-2014].

[11] Amazon. Sony playstation 3. `http://www.amazon.com/Playstation-3-250GB-System-Slim-Redesign/dp/B00AEX81SG/`, 2014. [Online; accessed 19-March-2014].

[12] Amazon. Sapphire Radeon HD4850. `http://www.amazon.com/Sapphire-Radeon-HD4850-PCI-Express-100245HDMI/dp/B001XW4BKO`, 2014. [Online; accessed 19-March-2014].

[13] Amazon. ATI Radeon HD 5770. `http://www.amazon.com/ATI-Radeon-DisplayPort-Dual-DVI-7120184001G/dp/B005EDG750`, 2014. [Online; accessed 19-March-2014].

[14] Amazon. Nexys2 500K Xilinx Spartan-3E FPGA development kit. `http://www.amazon.com/Nexys2-500K-Xilinx-Spartan-3E-Development/dp/B001D9EN6E/`, 2014. [Online; accessed 19-March-2014].

[15] Butterflylabs. The monarch BPU 600 C. https://products.butterflylabs.com/600-gh-bitcoin-mining-card.html, 2014. [Online; accessed 19-March-2014].

[16] Amazon.com. ASICMiner block erupter USB 330MH/s sapphire miner. http://www.amazon.com/ASICMiner-Block-Erupter-USB-Sapphire/dp/B00CUJT7TO, 2014. [Online; accessed 19-March-2014].

[17] Eurostat. Electricity and natural gas price statistics. http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Electricity_and_natural_gas_price_statistics, 2014. [Online; accessed 27-March-2014].

[18] Eurostat. Electricity production, consumption and market overview. http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Electricity_production,_consumption_and_market_overview, 2014. [Online; accessed 27-March-2014].

[19] Eirgrid. System demand. http://www.eirgrid.com/operations/systemperformancedata/systemdemand/, 2014. [Online; accessed 19-March-2014].