Bitcoin and the ASIC Conundrum

Written and Edited by: *Korbman*
August 20th, 2012

As many people know, Butterfly Labs Inc. has been producing custom field-programmable gate arrays (FPGA) specifically designed for the mining of Bitcoins.

The time is coming, however, when they are to be replaced by application-specific integrated circuits (ASIC), which is largely considered to be not only the next iteration in mining technology, but also the final frontier in hashing power before going Quantum.

At first glance, the idea is astounding; eye-opening, to say the least. Mining first began on the CPU, barely breaking into 1 Megahash (1 million hashes) per second (MH/s). Then came the introduction of the GPU and the surprising power that it holds, making Gigahashes per second (GH/s) a reality instead of a dream. And in recent months we've seen the push into FPGAs, thrusting us from 1-2GH/s into ranges 5 or more times that.

And we seem surprised that the next transition is to the upper echelons of GH/s and even the breakthrough to Terahashes per second (TH/s). That's one TRILLION SHA-256 hashes per second. For a year, it seemed only large mining pools had the capability to break this barrier. Now we're presented with the news that we can own this power on our own.

But is this too much power? How will the Bitcoin network react to such a drastic increase in speed? How will users react? What about the Exchanges and secondary markets?

It's extremely hard to answer these questions, and as a result all we can do is speculate. Looking toward the past won't be much of an indicator given the incredible volatility. And we all know looking to the future is nothing more than a best guess.

With a little digging, however, we can unearth some of these best guesses and see where it leads us.

Mining Pools and Their Top Hashers:

At the time of writing, the network hash rate sits at about 20 TH/s (varying by ±2TH/s every so often) and difficulty is 2190866 (set to increase 10.3% to 2416087 soon).

How are we managing to pull off **20TH/s**? The top 5 mining pools account for approximately 60% of all hashing power. These pools are:

1. DeepBit at around 3.7TH/s
2. EclipseMC -- 2.2TH/s

3. 50BTC -- 2.1TH/s
4. BTCGuild -- 2.1TH/s
5. Slush -- 1.5TH/s

NOTE: These rankings change all the time as workers come and go, stop and start. This information was obtained from: http://bitcoincharts.com/bitcoin/

I went through each of these pools trying to get an idea of who contributed the most. I wanted to see if I could figure out (or at least make an educational guess) what percent of miners were really behind the network hash rates we keep seeing fluctuate. To meet the 'top tier' requirements in my mind, the miner must be going at a minimum of 4GH/s (though I settle for 3.5GH/s).

DeepBit
There are roughly 7,200 (±500) workers associated with the various teams at DeepBit. 5,800 of these workers were situated in the top 45 teams (out of 750 or so), with the top team having over 1,200 workers alone.
When tallied up, these 45 teams (6% of the total) contributed 1.6TH/s out of the total 3.7TH/s (43%). In each team, roughly the top 3% controlled 70% (±5%) of all hashing power for that team.
TL;DR: 5,800 workers in the top tier of the pool, and 174 of them control 1.12TH/s of power (30% of total pool hash rate).

EclipseMC
Around 1,500 workers seemed to stay constant while I did my research. Out of these workers, the top 40 hashers made up 858GH/s. A nice 39% of the total pool's rate of 2.2TH/s, yet only 2.6% of all 1,500 workers.

50BTC
A bit more difficult to determine total workers, but my calculations put it around 2,700 (±200). The top **20** (!!) hold 829GH/s of power, compared to the total pool rate of 2.1TH/s. In this case, we're looking at **0.7%** of workers contributing 40% of the pool's power.

BTCGuild
This pool was nearly impossible to find statistics for. Given their total hash rate of 2.1TH/s, I'm giving my best guess that they have around 2000-2500 workers, so I'll say 2250 in this case (though please correct me if anybody has a more accurate number). Their top 50 miners (2.2% of total) still manage to contribute 709GH/s, or 34% of total power.

Slush
Lastly we find ourselves with the immensely variable BitcoinCZ Mining (also known as Slush), which I've seen go around 1.2 to 1.7TH/s throughout today. For easier calculations, we're going to assume 1.5TH/s is relatively accurate.

Although they have a reported 7,700 workers, they don't have any solid information on top contributing workers or such statistical data.
However, we can average the other 4 pools "top tier" percentages, which comes out to 39%. Meaning, the top 3% of miners (230 here) contribute 585GH/s (or 39% of the total 1.5TH/s).

When condensed, we find that the top 5 mining pools contribute 11.6TH/s (though let's round to 12TH/s) out of the total network rate of 20TH/s. Out of this 12TH/s, the top 3% of miners work to an astounding rate of 4.5TH/s, nearly **38%** of all power.

DON'T FORGET -- These numbers are purely educational guesses based off of data I gathered over the course of 12 hours (or so) on August 20th, 2012. This WILL change over time...probably will be obsolete by next week :P

The Network

The thinking goes, if you can get an idea for the top miners, you can get an idea of who will be controlling the network when ASIC mining hits full throttle.

As I noted before, I only touched on the top 5 pools, which was roughly 60% of the total network. So let's work out some math:
Added together, the top pools are supporting approximately 21,350 workers. At 60%, this would mean the total network is working with around 35,500 workers (I suppose ±2000 at this point).

With the averages above, we're looking at the top 3% of miners to see how many actually contribute in any substantial manner. At 3%...

- **DeepBit** contributes 216 miners
- **EclipseMC** -- 40
- **50BTC** -- 80
- **BTCGuild** -- 70
- **Slush** -- 230

...for a nice total of 636 'top tier' workers. Added up, these 636 contribute a solid 23% of all network hashes.

If you look toward the network as a whole, the top 3% comes out to about 1065 (out of the total 35500). The theory is...if you've invested this much time, effort, and money into achieving the status of "97th percentile", then the chances are that making the switch to ASIC devices won't require much thought.

Speculation and My Incoherent Ramblings

Welcome to the final section of my research, where even educational guesses can't predict the mercuriality of Bitcoin and the future of the network.

Yet I still feel compelled to try because the biggest question is still on my mind; Will Bitcoin still be profitable?
Yes! I mean, **no**. **Maybe**? **Hopefully**?

Let's *hash* it out and see where we end up. Let's assume my previous math was correct, my numbers are solid, and the percentage of top miners was accurate.

When the transition to ASIC devices is fully underway, I entirely expect to see a substantial drop in casual mining (workers going at around 300MH/s and under), which essentially accounts for about 60% of total workers (no math here, just pulled that number out of my ass to suit my idea of "best guess").
If the top 3% (1,065 workers) are equipped with substantial GPU and FPGA setups, I can only presume they're going to be the ones purchasing BFL SC Singles and "Mini-Rigs". This leaves 34,435 "casual miners" with standard GPUs.

But not all 1,065 workers will be making the BIG purchase to get a Rig. My thoughts for that reside within the Top 5% of this tier, or about 54 workers. So here's how it looks to me so far:

Normal	34,435
Singles	1,011
Rigs	54

When the transition is made and underway, invested users will stay by purchasing BFL SC 'Jalapeno' devices (for the most part, GPU mining is now obsolete). Upon losing 60% of normal workers because they can't compete with high GH/s and TH/s, we end up looking like this:

Jalapenos	13,774
Singles	1,011
Rigs	54

This would mean a vast increase in hashing power and difficulty.

Jalapenos	13,774	3.5GH/s	48,209GH/s	
Singles	1,011	40GH/s	40,440GH/s	
Rigs	54	1000GH/s	54,000GH/s	**142.65TH/s Tot.**

That's right, 142.65TH/s. A 7-fold increase in hashing power, accompanied by an equal increase in difficulty to approximately 15,336,055.

And to top it off, we see the reward split to 25BTC per block coming up.

1. Buy Rigs, 2. ???, 3. Profit

Each BFL SC "Mini-Rig" goes for a flabbergasting $30,274 ($29,899 + $348 Shipping).
With the new difficulty and reward split, the Bitcoin Mining Calculator shows an income of about 1,000 bitcoins per month. And I like to assume that Bitcoins are worth something around $5 (since that was when it was stable for the longest, though I'm willing to entertain the idea that the price will double to $10 during the reward split).

If the Rig pulls down 1,500 watts, you're looking at a usage of around 1,080KwH. In my area, at $0.147 per KwH this would be more or less $160 a month.

So $5,000 - $160 = $4,840 per month profit. Also known as a *6.25* month payback period, which is an extraordinary time (in a good way, I was expecting longer when I did my calculations).

Feasible? Seems that way. Practical? Not too shabby if you've got the money. Profitable? Eventually.

But if anything...nothing will change. The top miners will stay in their upper percentile as the majority of us fall to the wayside or buy up singles and Jalapenos to make up for our now lacking GPUs. It completes the cycle from MH/s to GH/s and moves us further into the world of Bitcoins. There will be turbulence to begin with of course, but when the market and network stabilize I imagine nothing will appear different.

Then again, I suppose that's just wishful thinking :)

Like this article? Feel free to donate mBTCs :)
153gA4XDZaenivE68SGZ4wXEcS4BgFobjY