ASIC Mining Analysis by Simulation

Alex Lee

(Originally published to Medium, 8/2018)

Whether ASICs are beneficial or detrimental to cryptocurrency networks secured through proof-of-work seemingly depends on whom one asks: while some will posit that ASICs are “bad” [1], others are happy to explain why they’re “great” [2], or simply want to pose the question for debate [3].

The crux of the issue appears to be the trade-off between security (as provided by more — and more stable — hashpower on the network) and decentralization. People generally want “more” of both of these things, though “more decentralization” is a fairly abstract concept when compared with “more security.” As such, how can we think about quantifying decentralization, and once quantified, can we make any assertions about the actual impact of ASICs on decentralization in a cryptocurrency network that uses PoW?

Quantifying Decentralization

There are surely several different methods for quantifying decentralization, but one fairly intuitive way is to examine a matrix which describes the percentage of network hashpower controlled by a percentage of miners. This is a bit easier to grasp visually — in an “optimal” scenario as far as decentralization is concerned, everyone has equal hashpower, and this matrix when graphed is a straight line at 45 degrees:

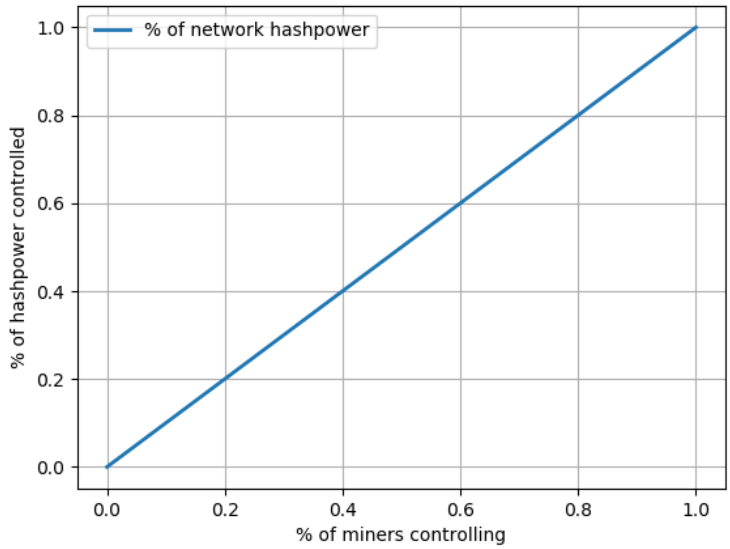

Figure 1: Even hashpower distribution under "ideal" conditions

If hashpower is less equally distributed, which is to say that “decentralization is worse” by our measure, the line will bend upwards. In the “worst-case” scenario where one miner controls, say, 99.999 percent of the hashpower, and the last fraction of a fraction of a percent is divided up among the remaining participants in the network, the graph would look more like a right angle:

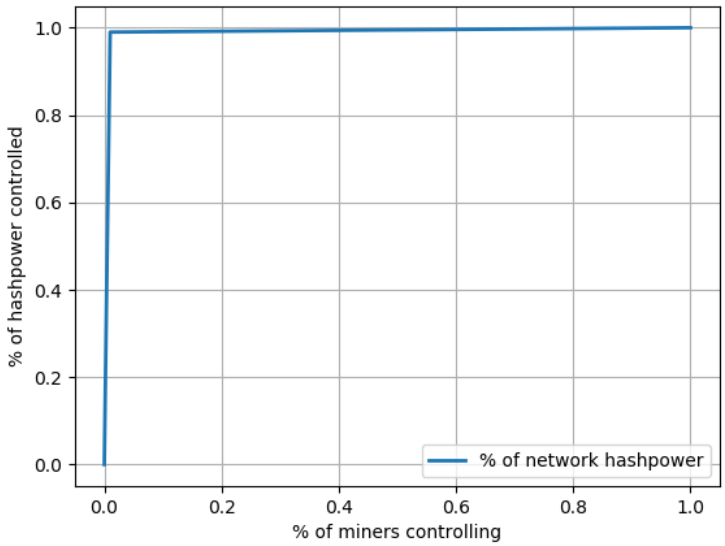

Figure 2: Uneven hashpower distribution in worst-case scenario

Given the matrix that such graphs describe, a single-point value for quantifying (de)centralization could subsequently be reported as the percentage of miners required to control, say, 95% of the network hashpower, in order to make the measure easily comparable across hypothetical cases, or, indeed, across actual cryptocurrency networks. (The full vector of percentages can also be used for comparison, of course.) So what impact do ASIC miners have on this particular measure of decentralization? We can attempt to find an answer via simulation.

Simulation Parameters

The simulation aims to capture two key aspects of a model cryptocurrency network with some degree of reasonableness: relative hashpower of hardware (an easier problem), and economics of running mining equipment (a slightly harder one). In attempting to reflect both of these aspects, the simulation instantiates a number of miners in a pre-specified ratio of ASIC miners vs. GPU-only miners — a panel can also be run over a grid of several different ratios, as will be shown below — and the miners are then given a random capital endowment to allocate towards hardware.

Hash power is parameterized on an index, with GPUs set at a base of 100. Using figures obtained from Bitcoin Wiki [4][5] this results in an index level of 28,000 for ASICs (using 50Mh/s as an approximation for GPUs in the sub-$600 range, and 14,000Mh/s as an approximation for high-end ASICs in the $3,000 range). These figures were not calculated with extreme precision, but I believe that they are reasonably realistic as ballpark figures — the code can also be easily downloaded and re-parameterized with different relative hashrates.

Economics are parameterized in two ways: prices for hardware (specified as $600 for a GPU and $3,000 for an ASIC), and budgets + spending patterns for miners who can afford one hardware type or the other. Budgets for GPU miners are drawn from a uniform distribution over the price range between a single GPU and a single ASIC, and budgets for ASIC miners are drawn from a beta distribution over the range of the

price of a single ASIC up to $100,000 (a fairly arbitrary cap, and distribution — again, feel free to re-run with different specifications).

When the simulation is run, a percentage split between ASIC and GPU miners is specified, then miner objects are instantiated with random budgets which are subsequently allocated to the hardware the miner can afford. For the results shown below, 500 simulations of a network with 10,000 miners were run and then averaged together for each incremental 5-percentage-point split between miner types (totaling 10,000 simulations). The resulting set of hardware-endowed miners provides a distribution over network hashpower, which can then be analyzed.

Results

First, let us look at a visual which mostly speaks for itself. The plot below is a surface made up of 2-D lines similar to those depicted above (you will notice two of the three axes are the same as in the prior graphs), under different scenarios in which ASICs are used by a different percentage of the overall miner population:

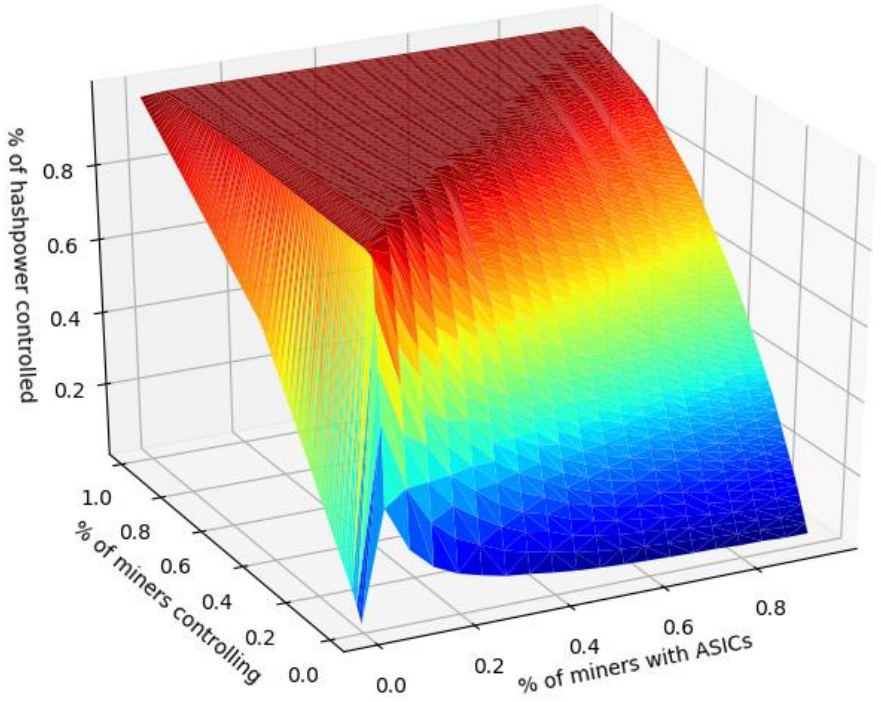

Figure 3: Concentration of hashpower under multiple scenarios, with different assumptions about the prevalence of ASICs in the network

What does this show us? The most obvious element of the graph is the sharp discontinuity in the surface when moving from a scenario in which 0% of the miners use ASICs to one in which just 5% do. (If you want to run this simulation yourself using the code provided, this percentage step size is a parameter you can play with.) This is due to the incredible efficiency of ASICs — using figures obtained from the Bitcoin Wiki, something on the order of 250x more effective than GPUs — so even a small percentage of the network using them swamps the hashrate overall.

We have immediately seen that once any miners start using ASICs, the distribution of hashpower becomes very highly skewed and decentralization (by our measure defined above) suffers — in the graph above, at 5% of miners using ASICs, the graph looks pretty close to our worst-case scenario. However, as a greater percentage of miners switch to using ASICs, the imbalance becomes less severe, and we move back closer to something resembling the "optimal" scenario. In the scenario depicted above where 95% of miners are using ASICs, the graph still bows upwards slightly instead of forming a 45-degree line; this is primarily due to the randomized nature of capital outlay in the simulation whereby a marginal ASIC "purchased" by a miner can skew the distribution of network hashpower more noticeably than a marginal GPU.

What do these results imply overall, then? We see that approximation of the "optimally decentralized" scenario is easiest when nobody has ASICs, but once anybody has them, everyone should want more people to have them in order to improve the state of decentralization of the mining network. If one is aiming for ASIC resistance with a protocol choice, they had better be quite certain that their form of resistance works, otherwise they will not only be missing their goal, but likely achieving its opposite.

Conclusion

This analysis is certainly not comprehensive with respect to every facet of the relevant variables of real-world cryptocurrency networks, and it also outlines just one approach to quantifying decentralization. That said, I feel this approach is both fairly reasonable and intuitive. Moreover, its conclusions are quite clear-cut if one accepts its definitions and premise: ASICs are probably good for decentralization, unless their use can be absolutely disallowed at the protocol level — a difficult guarantee to make.

Readers are encouraged to run the code themselves and play with the parameterization of the simulation — if any flaws are found in the code and/or additional interesting results are discovered, I would of course appreciate a response in the comments. Source code is available on GitHub at the following link: https://github.com/cs79/asic_sim

References

[1] "Why are ASICs bad?" (https://bitcointalk.org/index.php?topic=2192559.0)

[2] "Why ASICs are Great" (https://medium.com/neural-capital/why-asics-are-great-56d45496325e)

[3] "Are ASICs good or bad for the network?" (https://www.reddit.com/r/ZenSys/comments/8szcpx/are_asics_good_or_bad_for_the_network/)

[4] "Mining hardware comparison" (https://en.bitcoin.it/wiki/Mining_hardware_comparison)

[5] "Non-specialized hardware comparison" (https://en.bitcoin.it/wiki/Non-specialized_hardware_comparison)