Linzhi Semiconductors

Linzhi Working Papers
No 3

Achieving Mining Dominance. How Cost Advantage Drives Centralization.

by Sonia Chen

January 2019

Keywords: LWP3, Mining Dominance, 51% Attack, Centralization, Decentralization, Cost Advantage, Ethereum

Linzhi ASICs
Jan 12 · 5 min read

ASICs and 51% — Achieving Mining Dominance.
How cost advantage drives centralisation.

We want to take time to explain why we think a change in PoW is risky for Ethereum at this point.

First we need to understand how Bitmain achieved dominance in the BTC space. They did this through a combination of two things: Cost structure and luck.
Let's understand cost structure. When Bitmain built a miner the fact that they are the ASIC manufacturer gives them a cost advantage. For example, they could build a miner for 400 USD (300 of this is chips) and sell the miner for 1200 USD or more.
That pro t could be used in two ways: To build more miners and to mine BTC for themselves at a reduced cost. As luck would have it, they are also in China which gave them access to low priced power.
It's not the fact that they built an ASIC that gave them the cost advantage. If they built a GPU they would have the same cost advantage as an ASIC would.
It's the cost advantage vis a vis their customers that gave them the huge advantage and ability to dominate. Dominate in pools, and dominate in mining. Those early advantages multiply and the higher pro ts and lower costs allowed them to expand rapidly and gain control.
Now, of course, Bitmain is pretty much crushed as they own tons of inventory they can't sell and can't plug in. They have stopped building machines. They are no threat to ETH.

In the GPU space there are two companies who sit where Bitmain sat: AMD and Nvidia. By that we mean they can build mining rigs for the lowest cost because they control the GPU/ASIC *and* the memory. When you buy a graphics card for 400 USD, the real cost is actually 140 USD. Nvidia gross margin is 65%.

What separates Nvidia and AMD from Bitmain is *not* the kind of hardware they sell. GPUs are ASICs. What separates Nvidia and AMD is the following: Nvidia and AMD do not, as far as we know, self mine. They don't mine crypto themselves.

Currently here is how AMD (and Nvidia) sell: They sell chips and memory to a select number of distributors or board producers. These producers then resell the Nvidia product or AMD product. For AMD there are two such distributors.
These distributors mark the product up. If you want to buy directly from Nvidia and make your own cards you currently cannot. Same with AMD.
Why is this important? It's important because up to now all farms pretty much have to buy their cards indirectly at higher costs from distributors. And they have to compete with the gamer market.
Based on some previous discussions with GPU companies we know that they are open to working with large farms *directly*. For example, let's take Core Scientific, a large farm, or Genesis Mining, a large farm. Nvidia creates a graphics card for 140 USD, they sell it to distribution at 400 USD and distribution sells it at 450 USD. A large farm who buys from distribution pays 450 USD, just like everyone else. No problem. But what happens if the large farm does a deal with Nvidia or AMD? And Nvidia agrees to sell to them direct at 300 USD? In other words, what happens if Nvidia does a deal for example with large farms on the same terms that they deal with Dell, for example? What you get in this case is a strategic alliance that is effectively just like Bitmain. We know that large farms are out there seeking these kinds of deals. Deals with GPU makers that give them a cost advantage and it's that cost advantage that drives centralisation. If Nvidia can partner with a large farm they solve the problem of grey marketing of GPUs. We also know of farms that have tried to negotiate deals where they share the profits of mining back with the GPU or ASIC maker.

Is there proof of a relationship between Nvidia and Core Scientific? The issue is not proof. The issue is risk. We are pointing out a risk.
You won't find an agreement on the web between Nvidia and Core Scientific where Core Scientific is given preferential access to hardware.
You won't find proof that Nvidia sells Core Scientific product at a much reduced price in exchange for promotion of ProgPOW.
You won't find proof that Nvidia has offered Core Scientific specially tuned boards or specially tuned hardware or specially tuned memory.
You won't find proof that Nvidia agrees to sell Core Scientific parts that it has in excess at rock bottom prices.

You won't find any of this. The point is these things are all risks. They are known risks, and ProgPOW makes them even higher risks. With the existing PoW for ETH we are pretty confident that all the folks who buy

graphics cards are on a pretty level playing eld. And the cards have all been optimised and rmware optimised. With ProgPOW we have no such assurance. It's what we don't know that increases the risk. We don't know the relationship between Core Scientic and Nvidia, we don't know how tightly they are working together, and we cannot rule out an alliance that will have all the advantages that Bitmain had.
Core Scienti c has raised over 100M dollars, with top notch ex-Microsoft talent. Common sense tells you they would push for an alliance with Nvidia and AMD. And we have good intel that says they have such an alliance. An alliance that gives them a cost and technology advantage.
We have no proof, no copies of signed agreements between the two, but we see the risk. And the risk is larger than the risk that Bitmain or any other ASIC manufacturer can corner the hashrate on ETH.
This last point is what really confuses us. Bitmain and Innosilicon are dying, dying from competition with other ASIC guys. They pose no threat to ETH. So why would Core Scientic push for a change in PoW? Why risk a hardfork to protect against a threat (Bitmain) that has completely fallen down?
We think it's clear. Core Scientic and Nvidia have an alliance to give Core Scienti c and Nvidia an advantage in mining, just like Bitmain had.

We don't have proof, no secret company documents, but we recognise the risk. We recognise the risk because we competed against Bitmain for years and know exactly how they won. We see Core Scientand Nvidia as having the same opportunity that Bitmain exploited.

Costs of a mining GPU:

Typical mining die Nvidia GP104

GP104 mm2: 314
Usable wafer mm2: 65,000
GP104/wafer: 207
Wafer cost 16nm: <6500 USD

GP104 cost: <35 USD
4 GB memory: 40 USD

Cost for the mining GPU: 75 USD

The GP104 is used in many GPUs such as GTX 1060, 1070, 1080. To Nvidia, the cost of the die is always the same. Notice how GP104 dies are clocked between 810 MHz and 1607 MHz. The retail price of a GTX 1070 Ti is ca. 400 USD.

. . .

Never stop learning.
Linzhi Shenzhen
Telegram: https://t.me/LinzhiCorp