Statement of Wilke Trei (Lolliedieb) regarding BEAMs ASIC resistance at Mainnet Launch

Beam Network started January 3rd 2pm UTC. While everyone in the team was happy about the successful launch not soon after first comments arrived that the Networks hashrate is very high for a freshly started chain with new algorithm and some expected ASICs to be already dominating the network. At the time of this writing – which is Jan 5th, 3am UTC Beam network was reporting a total hash rate of 1,192,893.733 Sol/s on its modified Equihash 150/5 algorithm. Some point out that this is the equivalent of 100.000 Nvidia GTX 1080ti and higher and an enormous amount of hash power for the age of the network.

Overall these numbers are not wrong, they are indeed very impressive for a young network and we can not deny they are far outside of our expectations. Never the less we believe they must be seen in the right context.

1) There are not so many GTX 1080ti cards out there mining Beam.

With its hashrate of about 10 sol/s on the two reference miner implementations (the cuda is a little faster, the OpenCL a little slower) the GTX 1080ti cards are a easy way to make the abstract number of sol/s more tangible. But one often underestimates that AMD cards perform very well on BEAM compared with its Nvidia counterparts. Due to the limited time the team had to implement the reference miners – more on that further below – the code for CUDA miner and OpenCL follows the same strategy with the cuda miner copying the algorithm of the CL miner. This assertion can be easily verified having a look into the sources of the mining code at launch, see [1] and [2].

That said, the currently better performing options are often the AMD GPUs, e.g. the mid range RX 480 / 580 doing approximately 8.5 sol/s in both 4G and 8G variants (with smaller brothers 470 / 570 not performing much slower) or Vega GPUs performing at more then 13 sol/s. It is hard to find proper statistics about how many cards of which are used for mining overall. But following the statistics of the mining operation system ethOs [3] one sees that for this operation system the top 5 GPUs are dominated by AMD Polaris GPUs with first Nvidia Customer Card GTX 1070 at only 1/5 of the popularity of the leading RX 470.

2) Beam network is still big, not huge

Comparing the solutions rate of the Beam network with other PoW algorithms it was indeed one of the larger recent launches exceeding those of the Equihash 144/5 launches in summer 2018. That said considering the performance of the single cards being approx 1/3 of their Equihash 144/5 performance the total network hash is at the moment slightly larger then the combined GPU power of Bitcoin Gold (BTG) and ZelCash (ZEL) networks. Together these Networks have a combined hash of 3 Msol/s Equihash 144/5.

On the other hand the Ethereum network with its 171,000 Ghash/s rate has 40 times the size of beams hash rate when translated to RX 480 equivalent hash rates [4]. Considering that the rate was almost twice as large before the last reward reduction and the high attention Beam as the first Mimblewimble coin got its likely that many former larger scale Ethereum miners are currently mining Beam. If only 3% of those who left (!) the Ethereum network since summer will mine Beam now, they would hold the entire hash of the Beam network. And there will be others as well.

3) Its unrealistic there is a hidden ASICs testing in the background

Beam team has committed itself to give the GPU miners a head start planning two forks in the first year and doing an algorithm change away from the stock 150/5 protocol right from the start. When I joined the team to program the reference miner, which was December 14th 2018 the concrete algorithm change was not specified yet. In fact the team asked me to make a proposal and give me free hand with only restriction that it must be feasible to get it done and tested till launch.

I started by writing a standard Equihash 150/5 miner which completed on December 22nd in a testnet version. At this time the data path change was not specified. The idea for the actual change came later when studied the cuckaroo algorithm which will be used for Grins main network launch with its inventor John Tromp on December 23rd.

The change is very similar to those done in cucharoo and modifies the data path of the blake2b phase of the algorithm such that space-memory trade offs on ASICs and FPGAs are made much more costly [5]. The concrete approach used was first time presented to the team on December 25th, implemented on December 27th [6] and made public on December 28th.

Since this was only one week before the mainnet launch and the data path change would require a new chip design for the Blake2b part of the algorithm we are certain that there is no chip made it production ready in this time considering length of Hardware R&D cycles. Of cause within next month the possibility exists that specialized hardware – with a limited efficiency as described in [5] – will be created. Therefore the PoW scheme will be reviewed deeply in July this year and a fork of the scheme if scheduled to ensure an other few month where GPUs will be the dominating mining devices for mining Beam.

That all said – I am personally happy with the main networks start and look forward to see the ecosystem of Beam growing the next month. Happy Mining and a happy new year 2019.

Lolliedieb

References:

[1] Cuda sources of Reference miner at mainnet launch
https://github.com/BeamMW/cuda-miner/blob/a679e07ba00ff79ff5030b38c71cb4d72d68c2e3/equihash/cuda/CudaSolver-150-5-L.cuh

[2] OpenCL sources of Reference miner at mainnet launch
https://github.com/BeamMW/opencl-miner/blob/7150ac8580b4ae5293dd973bbb2a907196ae6893/equihash_150_5.cl

[3] Distribution of EthOs versions and running GPUs
http://ethosdistro.com/versions

[4] Ethereum network historic hash rate
https://etherscan.io/chart/hashrate

[5] Beam Algorithm Specification
https://docs.beam.mw/Beam_Equihash.pdf

[6] OpenCL reference miner commit implementing data path change
https://github.com/BeamMW/opencl-miner/commit/20605cdaa3d0e7ab9651f20184f241c306cbbd20