To Fork or not To Fork, that is the question.

I suggest that all further discussions on the ASIC topic be taken here, since things have been getting out of control trying to monitor github, twitter discussions and reddit.

Introduction

For the people that have not been following the news, it is now confirmed thatBitmain is selling an Ethereum mining ASIC. This can be potentially harmful for Ethereum's decentralization and thus the community is currently discussing on how this should be approached, potentially through a hard-fork change in the hashing algorithm used to achieve consensus.

There are valid arguments on both sides. I'll refer to bits and pieces I have extracted from my reading and understanding so far. This is where we should discuss with concrete arguments on each case.

My assumption is that full PoS, and not PoW/PoS Casper with epochs, is not close enough to be considered a remedy.

Ideas for the Fork

- X16R
- Elliptic Curve Exponentiation
- Modify ETHASH_CACHE_ROUNDS/ETHASH_ACCESSES
- 3 tiers of changes
- Change the FNV constant

Things to Consider

- The exact specs of the ASIC are not known yet (to my knowledge). As a result there is the "risk of switching algorithms only to find it that it didn't cripple the ASIC miners curretly in production" [1]. A proper fork must

force a new R&D cycle.(This starts to sound like a conspiracy)

- The E3 is approximately equivalent to a 6 1070 card rig, is around 10% more energy efficient and costs about a third of the price (correct me if I'm wrong here)
- Fluffypony says it takes 5 months from design to delivery
- Rushing PoS is not a solution, if not properly done it can be even more centralized than PoW networks which have ASICs.
- You cannot 'fire' miners, they are the ones who secure the network. Miners leaving Ethereum makes the network more vulnerable to 51% or censorship attacks. (relevant comment)
- GPU Miners are incentivized to be pro fork
- Bitmain clients are incentivized to be against the fork
- Is this really Bitmain's final form? Did they start selling this ASIC with mediocre

specs and are already mining with the next model?

- People who are actively working on the workarounds should be checked not to be linked to Bitmain as there is a conflict of interest (this is definitely a conspiracy)

Useful Links

- Ethereum Difficulty Chart
- ASIC Cost Calculator - for the people who actually know how VLSI design is done properly, unfortunately I don't (blame my professors)
- EIP 958 - Modify block mining to be ASIC resistant
- EIP 960 - Meta: cap total ether supply at ~120 million

- Let's talk about ASIC mining
- FPGA/ASIC Analysis

Things to avoid

- Assumptions without concrete proof, i.e. "There are X TH of Bitmain Miners" due to the recent hash rate increase. Correlation does not imply causation.
- FORK!!!1
- DONT FORK!!! POS WILL COME
- F*CK BITMAIN

My opinion:

First of all, let's not talk about Bitmain like it's the big-bad guy, it's a for-profit company and if that makes them money, they'll do it and profit very well from it.

It's not just the overhead from the actual development of the algorithm that will be ASIC-resistant. The biggest overhead will be firstly in coordinating and communicating the exact spec to all Ethereum implementations, and after it is developed ensure that it does not break consensus.

I believe that centralization risk is less than the risk of changing algorithms, let alone the workhour investment this task requires.

The wisdom of the crowd usually glosses over these 'nitty-gritty' details which are more critical than showing Bitmain the middle-finger.

I'll quote this from @phil's post: "Avoid the governance headaches and wasted developer hours, ending in the same economies of scale with likely more centralization."

I do not believe that playing cat and mouse is sustainable in the long run. If anything, we should be focusing our research hours on PoS and ensuring that it won't become centralized around stake.

I'm also very interested in hearing the expertise from people who have worked on VLSI systems.

Further thoughts

- How much more 'centralized' Ethereum can really become? In this paper it is argued that even a Byzantine Quorum system of 20 can achieve better decentralization than Bitcoin/Ethereum at their current state. Will the potential centralization from ASICs make things that much worse? OTOH, the increased hashrate from ASICs can make the network even harder to be attack.
- Would introducing an issuance curve so that we cap out at some amount of total Ether as per Vitalik's latest EIP discourage miners?
- Would going for an 'adaptive' consensus algorithm bring back FPGA miners? Just a wild idea that might be totally wrong.
- If a company can disrupt the status quo just with an ASIC chip, what happens if a nation state wants to play?