

**Subject:** Linshi PoW Feedback  
**From:** Sonia Chen <sonia@linshi.io>  
**Date:** 1/9/2019, 4:10 PM  
**To:** hudson@ethereum.org

Hudson:

### ---1 Introduction

We would kindly ask you to make the following people aware of this long mail (sorry it's long, but we think necessary): Martin-Holst Swende, Alexey Akhunov, Afri Schoedon, Pawel Bylica, karalabe, Jacek Sieka, David Vorick if possible. David is the #1 independent chip expert in crypto you can trust. We disagree with him on many things, but if you trust noone (you should not), start with him.

Add whoever you like, but we specifically ask you to EXCLUDE anyone from the ifdefelse Nvidia team, for reasons stated below. The mail is written in such a way that if it leaks, that's not a drama either.

We will try to confirm with you that the people listed had a chance to read it if they like, that's all we are asking for. Noone can complain later. We put our full effort into this.

### ---2 Recent Telegram Chat

We had a nice short chat between Hudson, David Vorick from Sia, and Chen Min from Linshi. No guidelines from Ethereum leadership have been issued yet. Questions remain unanswered:

Chen Min's questions:

- Why is an algorithm specifically designed for a chip good, but a chip designed specifically for an algorithm is bad?
- If an algorithm is designed for a specific manufacturer's well patented chip like a GPU, isn't that a monopoly already?
- If devs think some hardware is bad, what is the problem? Transparency? Performance?
- If hardware is deemed to be good, what is the standard? Programmable? Easy to buy?
- Is it reasonable to request that all hardware has the same cost, performance, efficiency?

David Vorick responded saying

"Public, clear guidelines from Ethereum leadership on what constitutes good behavior and would protect a manufacturer from being bricked would be extremely helpful."

### ---3 Ethereum Yellow Paper

We believe a crisis in Ethereum PoW is unfolding. The Ethereum Yellow Paper from 2014 has many non-nice

things to say about mining.

We think significant parts of section 11.5 are outdated and need to be revised.

We believe two key concepts are missing from 11.5:

1) well-being of miners

For as long as PoW exists, Ethereum software developers are responsible for the well-being of miners. A miner advisory board is to be setup that includes representatives from small and large miners.

2) PoW algorithmic predictability

PoW is cryptographically and thermodynamically provable. The playing field for chipmakers is leveled by announcing any change to PoW 2 years in advance, and leaving each chosen PoW activated for at least 2 years.

---4 Emergency Response

- Do not allow ProgPOW (Nvidia) to divide the Ethereum mining community into Bitmain and Nvidia miners.
- Reject ProgPOW for all times. They tried to subvert Ethereum and are banned for life. Nvidia is worse than Bitmain.
- Bring most miners that are asking for ProgPOW back into the team by increasing block rewards.
- Expect a massive Nvidia attack against this of the kind you have not seen before. Prepare for this attack and fight back. Learn something about chip business and marketing.

---5 Thoughts

The advance notice of 2 years removes most incentive for chipmakers to influence selection of PoW algorithm, in ways that may be beyond the visibility of Ethereum software devs. Even with the 2 year window in place, changes to PoW must be carefully and independently researched by impartial Ethereum developers only.

The PoW algorithm distributes money. Developers involved in PoW changes must wisen up on this and build their own chip design and manufacturing competence team.

Commodity hardware is more susceptible to insider games, for economic reasons. Forecasts may be wrong, defective lots, quarterly sales pressure, pressure from competitors, tuning/throttling/binning/etc.

All invisible and very hard to quantify things. Specialized hardware is more stable economically and computationally.

---6 Our Nvidia Story  
Fasten your seat belts.

In Q1 of 2018, when mining looked ultra profitable, Nvidia decided to capture more of this market. It was approved at high levels of Nvidia like any other serious market entry.

They would do all the normal things they have been doing for decades. Attack competitors, exclude competitors, focus on money flows, understand buying cycles, create great stories that would make people want to buy their stuff.

Miners would be turned into gamers, to be given as much as they need, with all other money flowing back to Nvidia.

After some work, ProgPOW was conceived as a way to exclude Bitmain and give Nvidia a way to tune chips for big mining partners, with revenue sharing back to Nvidia.

ProgPOW, if activated, will be a nightmare for Ethereum. It will tilt the table towards Nvidia. Large miners with special deals with Nvidia will benefit, together with Nvidia itself. Independent miners become gamers, sheep. ProgPOW ASICs will be made and then Nvidia will attack those. We are ready for this fight (with Nvidia), but if the price is the destruction of the Ethereum community, that may be acceptable to Nvidia, but unacceptable to us. No worries about us, everyone wants to buy ProgPOW ASICs. Even today the very same people that are saying it cannot be made tell us, if we can make it, they will buy.

Ethereum developers, whether you like it or not, are competing with Nvidia for the miners. Nvidia will try all they can to sell their chips to the miners, you need to compete and you are not used to this kind of competition. You control the block rewards, so if you are very forceful in your message, miners will understand that you, the Ethereum Devs, are taking better care of them than Nvidia. Nvidia however will not be happy that you don't care which chipmaker those block rewards are going to. They will try to educate miners that it's best if mining happens on Nvidia... The question is whether you are selling out to Nvidia pressure, and allow Nvidia to take the mining market and turn it into a normal game-like market for them. With ProgPOW you would be choosing convenience over security.

We can imagine these are stories from a world very foreign to your developer world. Nvidia is a machine to make money. Nvidia is hungry for money. They identify markets, they define products, they compete and try to capture as much profitable revenue as they can. Don't sell out to Nvidia. Ethereum will be greatly damaged from this in the long run, because the technical foundations of ProgPOW are laughably weak, just fantasy marketing

stories.

If you cannot stand Nvidia pressure, switch to PoS immediately!

Maybe you can find independent game review journalists (if there are any independent ones left), and ask them about Nvidia competitive tactics. Ask them how they enter markets, kill competitors, etc. Some of what you hear may sound familiar to you by now :)  
When fiddling with PoW, never allow one chipmaker to give you "advice". Don't allow any chipmaker to stir up your miner community to demand exclusion of competitors.

If ProgPOW is activated, the resale value of GPU rigs may go up one last time.  
IMPORTANT: The Ethereum developers should advise all miners to sell their GPU rigs at that time!  
The ones that will listen to this advice will be better off than others. From then on there will be an unstoppable decline in value of GPU rigs because independent miners are hurt from Nvidia back dealings which they can never compete with. Either Nvidia takes the money, or new ProgPOW ASIC makers take the money.

A small rant about dev call #52: Are you guys all completely out of this world to invite Nvidia marketing people into your developer call? You obviously do not understand at all how they work.

It's painful to listen to "Mr Else" destroying technical arguments, and directly lying to Martin's (and others) faces.

Who is "Mr Else"? They say he is anonymous because "great work should stand on its own technical merits, like Bitcoin" (!). They are so arrogant to think that they can even use our own principles against us.

So Martin is standing there with the full reputation of his real name, and takes advice (!) from an anonymous Nvidia marketing guy telling him lies? Not lies of course, "sales stories" that further Nvidia's cause.

Are you drilling into these people's backgrounds? Real names. Employers. Where do the ProgPOW sources come from? Who are the engineers that wrote them?

Who has reviewed the "open source" ProgPOW?

Why are the commits from the "anonymous team ifdefelse"?

Since when do free software people accept large blocks of code from unknown origins, filled with math, algorithms, magic constants? This is fake open source code, with any amount of performance backdoors, held-back optimizations, intentional throttling, etc all there and noone but Nvidia knowing.

I am sure you guys have thought through every line of code, understood the reason behind every magic constant. You must have.

Or you believe the stories "Mr Else" is telling you?

We are holding some small hope that Nvidia can be stopped.  
Maybe they miscalculated the opportunity this time.  
Crypto is not just another game.  
We are proud to be a small 10-person independent chip  
company in Shenzhen with 0 revenues that is fighting back.  
We are too small to be attacked by Nvidia today, we have  
no revenues that they could try to steal.

No matter how ProgPOW continues, in a year we are all wiser.  
After this drama is over, I hope good people will have learned  
something, and we will exclude Nvidia from anything Ethereum  
forever. By then Nvidia will have proven to be worse than Bitmain.

Good luck!  
Linshi Shenzhen Team