Linzhi Semiconductors

Linzhi Working Papers
No 2

Call to Ethereum Developers for ASIC Guidelines.

by Sonia Chen

January 2019

Keywords: LWP2, ASIC Guidelines, News, Ethereum

Linzhi

Linzhi Shenzhen Co., Ltd
深圳凛炙电子科技有限公司

Shenzhen, January 8, 2019

***** Call upon Ethereum Developers *****

*****Publish rules for what constitutes a good ProgPOW ASIC maker *****

*****呼吁以太坊开发者公布 ProgPOW 算法对合格 ASIC 制造商的规则 *****

Linzhi is an independent, privately owned and self-funded fabless semiconductor company headquartered in Shenzhen. We have no affiliations with other semiconductor companies, and are a small team of about 10 full-time employees.

We make chips for Ethereum because we believe in Ethereum and Proof of Work. We design for Ethereum, for better efficiency and better performance. We are not attacking things we believe in, and are currently designing an Ethash mining machine. [1]

We were shocked that Ethereum developers would consider teaming with one hardware company, and surprised they would rush a solution that burns 8 times the energy when miners are already having their reward cut. [2] We reject arbitrary enforcement of rules, and request clear and equal guidelines to be established for all hardware makers.

Today we are calling upon the Ethereum developers to publish rules and requirements for what constitutes a good ProgPOW ASIC maker. It would follow the methodical approach of Ethereum developers to agree upon and release such rules before ProgPOW is activated.

在此，我们呼吁以太坊的开发者们，公布 ProgPOW 算法下对合格 ASIC 制造商的规则和要求。
我们呼吁以太坊的开发者们，遵循他们的一贯准则，在 ProgPOW 算法激活之前，能就此达成一致并公开这些规则。

Linzhi Team, Shenzhen
Telegram: t.me/LinzhiCorp
email: sonia@linzhi.io

[1] https://www.coindesk.com/a-multi-million-dollar-bet-ethereums-proof-of-stake-isnt-coming-soon
[2] https://www.coindesk.com/ethereum-developers-give-tentative-greenlight-to-asic-blocking-code

Ethereum Miner Linzhi Calls Out Project Coders for Proposed ASIC Ban

Rachel Rose O'Leary ☐ ☐

☐ Jan 8, 2019 at 14:00 UTC Updated Jan 8, 2019 at 15:38 UTC

Shenzhen-based miner manufacturer Linzhi has published a statement in response to a “tentative” decision, made by ethereum developers Friday, to block specialized hardware, or ASICs, from securing the platform in exchange for rewards.

This would involve the implementation of “ProgPoW” in an upcoming upgrade, a code change that is optimized for graphic card, or GPU, hardware.

In today’s statement, Linzhi said it was “shocked” by the move, stating, “We reject arbitrary enforcement of rules, and request clear and equal guidelines to be established for all hardware makers.”

The statement continued:

> “Today we are calling upon the ethereum developers to publish rules and requirements for what constitutes a good ProgPoW ASIC maker.”

Elaborating on the statement in an email to CoinDesk, director of operations Wolfgang Spraul said that such rules could include more transparency, or even monthly audits of hardware companies by ethereum developers.

“The rules should probably include defining better relationships between hardware makers, miners, and developers,” Spraul said, “That’s up to the ethereum developers to define, we think.”

Following the meeting on Friday at which the developers approved the proposal, discussion regarding ProgPoW has escalated, with several prominent community members coming forward to argue against the change.

ASICs for ProgPoW?

Linzhi is currently designing a chip for ethereum's current mining algorithm, Ethash. Having expended $4 million on its production, the upcoming miner claims significant advantages over former ethereum ASIC designs.

In conversation with CoinDesk, Spraul also said that pending its implementation into ethereum, the company will research the feasibility of building specialized ASIC hardware for ProgPoW.

"I can publicly confirm today that we intend to study the feasibility, and then build, ProgPoW ASICs," Spraul said.

Because ProgPoW changes ethereum's underlying mining algorithm, Ethash, to be more memory-heavy, the code switch is said to make GPU hardware competitive with ASICs.

Proponents of ProgPoW say that if hardware designers try to build ProgPoW ASICs – which is to say a specialized chip with the sole function of computing ProgPoW – it would just end up resembling GPU hardware.

Still, Spraul denied this, stating that "Hardware innovation is non-linear," and "We can accelerate ProgPoW by a factor of 3x to 8x."

Yesterday, ethereum classic underwent a 51 percent attack – something that the cryptocurrency's Twitter account claimed may have come from Linzhi. Spraul pushed back on such claims, saying "They are entirely baseless."

ASICs Mining Ethereum ProgPoW Linzhi

Linzhi Ethash Miner – Telegram https://t.me/LinzhiCorp
8 January 2019

Background: Ethereum Miner Linzhi Calls Out Project Coders for Proposed ASIC Ban
https://www.coindesk.com/ethereum-miner-linzhi-calls-out-project-coders-for-proposed-asic-ban

17:51 Hudson Jameson

@LinzhiAdmin I'm from the Ethereum Foundation and a Reddit moderator. I can help you approve your post on there if it is not already approved.
Why hasn't Linzhi reached out to any core developers or the Ethereum Foundation before releasing your statement today?

18:02 Sonia Chen

we are assuming noone will listen to us

18:02 mAhOf

Linzhi was interested in chips yesterday today marketing came after etc (my opinion)

18:02 Sonia Chen

@Souptacular who can we contact in the future?

18:03 Hudson Jameson

You can contact me and I can put you in touch with who you need to speak with depending.

18:03 Sonia Chen

@Souptacular thank you very much!

18:03 Hudson Jameson

It seems you are not in tune with the Ethereum community or the anti-ProgPoW people if you assumed no one would listen and didn't even make an attempt.
To be honest your statement seems like a marketing ploy.

18:06 Min Chen

Hi Hudson, I am chen min from linzhi, thank you very much to help us reach out ethereum dev team

18:06 Hudson Jameson

Absolutely. Happy to help.

18:08 Min Chen

we'd love to talk/work with dev team, just didn't get right path before

the motivation we start linzhi in first place is: we believe hardware have a lot possibility to contribute on blockchain performance/efficiency

18:13 Hudson Jameson

In your "Call Upon Ethereum Developers" you state that rules and requirements be published for a good ProgPoW ASIC maker. What does that mean and what is an example of a rule/requirement you would anticipate?

18:57 Min Chen

In linzhi's perspective. Most hardware is specially optimized for a certain target.
CPU is a chip that specially optimized for execution an instruction set.
GPU is a chip that specially optimized for graphics processing.
Linzhi's lavasnow is a chip that specially optimized for ethash acceleration.
Hardware manufacturers profit by providing better efficiency/performance/reliability on what it optimized for.
Semiconductor foundry not offering free silicon wafers. CPU/GPU manufacturers also not non-profit organizations.

So we are interested in why developers don't like "a chip that specifically for an algorithm", but "an algorithm that specifically for a chip" is acceptable, like ProgPOW for GPU.
For a public algorithm, people are open to competition with cost/performance/efficiency. maybe some moment one vendor is big. But in others catch up soon in months. no single player can easily control the network in long run.
If an algorithm is already designed for specific manufacturers' well patent chip like GPU. There are already monopoly.

We want more clear standard on how Dev team choosing those things.
Predictable is very important.
If Devs think some hardware is bad, what is key problem? transparency? performance?
If some hardware is good/welcome, which standard is it. programmable? easy to buy? we are happily working to meet that requirement.
Assuming every hardware have same cost/performance/efficiency is not realistic, it looks like require every software developer have same knowledge/skill.

19:05 Sonia Chen

wow! thanks @Souptacular for opening this path of communication. To make this clear, Chen Min is our founder, and sole owner of Linzhi. She designed all successful Avalon SHA-256 chips since 2013. We are a distributed team, and if she writes this here it's news for us in the team as well. Happy to work with Chen Min, Hudson, and everybody else who gives input.

19:08 David Vorick

Can speak as an independent: Ethereum appears to most hardware manufacturers to be very hostile
The move to break the current eth ASICs is generally viewed as a sign that eth has the potential to break any hardware that gets released in the future
Building a chip takes lots of time and lots of money. Even a 10% chance of having your hardware bricked is very material, and uncertainty drives manufacturers to heavily prefer secrecy
Public, clear guidelines from Ethereum leadership on what constitutes good behavior and would protect a manufacturer from being bricked would be extremely helpful

19:11 Kristy-Leigh Minehan

Of course.

19:12 Jon Phillips

"So we are interested in why developers don’t like “a chip that specifically for an algorithm”, but “an algorithm that specifically for a chip” is acceptable, like ProgPOW for GPU."
Well put!

19:15 Guy Corem

If I need to guess, the devs believes that Nvidia / AMD are trusted to play fair, sell to everyone and not self mine

19:15 Jon Phillips

Really? haha!

19:17 Min Chen

If Devs decide choose AMD/NVidia as official parter, that’s also perfect but better to be declared.

19:35 Kristy-Leigh Minehan

Sorry guys, day job calls. we will respond to the ETH magicians thread and if the guideline is to help synergize ETH with HW manufacturers we will help and do this as well.

19:35 Hudson Jameson

Thank you for answering @chenmin_ac!
Hi @Taek42. Nice to see you here.

19:40 Jon Phillips

Thanks Guy! I'm reading about NVIDIA and AMD. The two CEO's are related!

19:41 Kristy-Leigh Minehan

What o.on

19:44 Hudson Jameson

To answer @chenmin_ac, my understanding of this issue is from my conversations with core developers because my knowledge of this topic is limited. They seem to believe that there is a possibility for hashpower centralization from manufacturers of ASICs (I understand a GPU is an ASIC, but for the purposes of this conversation I will use the term ASIC to refer to specialized miners such as the E3 that are not normal GPUs used for gaming). The reason for this is because of evidence of secret ASIC mining on profitable coins like Monero have been arguably discovered. Because there is a switch to PoS in the next 1-3 years, it is ideal to reduce the chance of hardware centralization.

Another point made is that by ensuring mining on commodity hardware is cost effective, we lower the barriers of entry, ensuring better decentralization and reducing the likelihood of a contentious fork since commodity miners can just pivot their miners to a new chain without losing their hardware investment.

19:45 Kristy-Leigh Minehan

Oh yes, let’s talk about the XMR secret mining.

19:47 Hudson Jameson

@Taek42 independently speaking on my own behalf: I'm not convinced we need ProgPoW and I don't believe Linzhi has malicious intent. However, companies and people do operate in their best financial interest and so I can never be sure of the intentions of a company are to be malicious and gain majority hashpower secretly. The secret mining on the Monero blockchain and Bitmain's secretive agenda don't help the case for other ASIC manufacturers and causes trust issues on both sides imo.

19:48 David Vorick

My understanding is that monero was mined in secret because of their heavy asic-resistant stance. If they had not been an asic resistant coin, they would have had public machines.

19:48 Hudson Jameson

Ethereum is suppose to be ASIC resistant according to our white paper.

19:48 David Vorick

Yes, which drives manufacturers to secrecy

19:49 Hudson Jameson

I agree. So it is an unfortunate reality.

19:49 Kristy-Leigh Minehan

I’ll be answering any questions about ProgPoW in the ETH classic voice chat on Discord.
Feel free to come ask. Voice is easier while fighting fires.

19:50 David Vorick

Money ends up driving everyone at the end of the day. The amount of money at stake is career breaking for many of us, that limits our options sometimes.
So it is best to think of the game theory as profit maximizing, even for ideological individuals

19:50 Greerso

Everyone knows that a purpose built ASIC can outperform general use hardware like a GPU. ProgPoW makes the most of a GPU, this does not prevent ASIC's, it just means that ASIC's will not be able to monopolize the network. This point goes to the claims that ProgPoW gives a monopoly to

AMD/Nvidia, it does not. All manufacturers can develop hardware to mine ProgPoW extended ethash, they just cannot monopolize the network hash as they would wish to.

19:52 Hudson Jameson

The ideal scenerio would be for ASICs to be developed using open source specs for the community from.the get-go to prevent secrecy and maximize transparency, but at this point that cannot happen.

19:52 David Vorick

Developing a gpu with comparable performance to what nvidia can do is a massive task, well out of reach for startups and even more well funded companies

Why not?

19:52 Hudson Jameson

Because Linzhi already spent money.

19:52 David Vorick

If you are changing pow anyway, you can change the pow to something else

19:53 Min Chen

It is 3AM in Shenzhen and I need to sleep, I will reply everything tomorrow.

19:53 Hudson Jameson

Goodnight! Thanks for the open dialogue Min Chen.

19:54 David Vorick

Linzhi is at risk of losing everything depending on the decision you make, my guess is that you could bargain for open source chips
(that's not me speaking on their behalf)

19:55 Hudson Jameson

Interesting idea. The main issue is that even though it would solve the problem for Linzhi, other manufacturers like Bitmain are or may be operating in secrecy.

19:56 David Vorick

Yes, but one open source spec is better than you will ever get close to with gpus
Gpu firmware isn't even open source

19:56 Kristy-Leigh Minehan

Not true.
At all. It’s under NDA and ConsenSys would have access to it.
an ASIC manufacturer could have access to it.

I still stand firm that ProgPoW can standardise hashrate across all hardware implementations.
And thus is a good fit for both ASIC and GPU and FPGA.

19:57 David Vorick

Being able to access the firmware is not the same as FOSS, which is generally what I mean when I say open source

19:57 Greerso

Linzhi have claimed that they can do it for ProgPow. Also, Linzhi knew ProgPoW was a very real probability back in September and bet against it. It is still a free market.

19:58 Kristy-Leigh Minehan

There is a lot of FUD about how ProgPoW works and no one realises it is about balance and equality across all hardware types.

20:00 Hudson Jameson

This is true if we were continuing to use PoW indefinitely. Since we are moving to full PoS it is less important.

20:00 David Vorick

Then why fork at all? Is there evidence that the correct hashrate is highly centralized?
Has ethereum done an exploration on the major eth mining farms and how much hashrate each has?

20:01 Hudson Jameson

Not sure. I wasn't heavily involved in the research of ProgPoW.
I know the 2 largest farms myself that represents about 50-60% though.
Apparently the majority of core devs believe that there is enough risk that it is worth forking to a new PoW as a temporary measure before PoS.

20:02 David Vorick

Are those GPUs or ASICs?

20:02 Hudson Jameson

GPUs.

20:03 Jon Phillips

Where are NVIDIAs chips made?

20:03 David Vorick

So doesn’t bricking all the ASICs make that worse?

20:03 Hudson Jameson

Make what worse?
The centralization?

20:04 David Vorick

TSMC. The expensive part is not the tape-out it's the design. GPU chips are comparable in complexity to millions of lines of software code

20:04 Jon Phillips

Can chips be opensourced that TSMC makes?

20:04 Greerso

current eth asics are already obsolete as proven by linzhi claims. Also, fnv is exploitable by fpgas

20:04 David Vorick

If the two biggest farms are GPU and represent 60% of the hashrate, and you brick all ASICs, the hashrate will go down but the GPU farms will have the same hashrate, bringing them above 60%

20:05 David Vorick

Depends on how much you are open sourcing
For digital designs you can open source the core IP
For analog designs it's a lot messier

20:05 Hudson Jameson

Those 2 biggest farms are altruistic and won't attack the network. I'm personally sure of it, but obviously I can't be 100% sure.

20:06 Jon Phillips

@Taek42 so you cannot 100% open source the chip?

20:07 David Vorick

Depends on where you draw the line for 100%.

20:07 Hudson Jameson

In my ideal world I'd rather have 2 major farms who I know won't attack the network, then secretive mining companies who can discreetly deploy a ton of hashpower suddenly who do not have previous connections and relationships with the network and it's participants.

20:07 Jon Phillips

Ok, so no. Not possible to have open source chip made at TSMC.

20:08 David Vorick

This is wrong
90% of chips have a digital process as their core IP and can be open sourced
Giving a gate-level description of a chip is far better than saying 'oh no can't open source the full manufacturing process so it's not open source'
By that logic, no hardware can be open source
Is the PCB open source? Oh it's got capacitors on it, are they open source? Well, they were manufactured somehow, are those machines open source? What about the manufacturing process behind those machines, turns out those machines have their own capacitors, etc

20:12 Jon Phillips

Any rough % of business for NVIDIA at TSMC (Taiwan Semiconductor Manufacturing Company)?

20:14 Hudson Jameson

I have to go for now. Thank you for the conversation @Taek42. Made me think about my personal position more.

20:15 David Vorick

One last parting remark
Nvidia is just as capable of spinning up massive hashrate as Bitmain is
They already charge customers different prices depending on application for some of their ML and big data clients
No reason that can't do that for crypto as well

20:17 Hudson Jameson

Interesting. I've never thought about that.
Later!

20:18 Jon Phillips

Whoa, AMD has chip production at TSMC too.
Oh man, you are fueling digging! Thanks for the knowledge.
Looking for this...

20:28 Sonia Chen

I think we have come to a temporary break. Wonderful conversation with important arguments. What I would like to do is to look at a transcript of the key points, to see whether that makes sense. I would only publish this anywhere if there was at least tacit agreement for this being valuable. I don't want to harm our ability to speak freely in the future, but I also want to recognize the fact that this group chat is semi-public and may have value beyond the moment of conversation.