

# Linzihi

Semiconductors

## Linzihi Working Papers

No 6

### Bridging the Hardware- Software Divide.

by Sonia Chen

February 2019

Keywords: LWP6, Hardware-Software Divide, Bridge, ASIC, Ethereum

This publication is available on <https://linzhi.io>  
Telegram discussion <https://t.me/LinzhiCorp>

All original rights for text and media are released into the public domain, attribution welcome. Rights of quoted or translated sources remain with their respective owners.

# Bridging the Hardware-Software Divide: 4 More Claims.



Linzi ASICs

Feb 3 · 3 min read

Linzi Ltd. is a private fabless semiconductor company in Shenzhen. On January 8th, we called upon Ethereum developers to publish rules and guidelines for what constitutes a good ProgPoW ASIC maker. <https://www.coindesk.com/ethereum-miner-linzi-calls-out-project-coders-for-proposed-asic-ban>

Today Alexey Akhunov published a wonderful opinion piece with 4 claims, which we see as a massive effort to bridge the hardware-software divide.

<https://medium.com/@akhunov/my-take-on-progpow-looking-for-a-reasonable-answer-to-a-reasonable-question-9f13ffd4e9d7>

The Qi Hardware community provided a Chinese translation of Alexey's claims:

<https://qihardware.org/2019/02/03/my-take-on-progpow-chinese.html>

To respond, we first quote Chris Ziolkowski, founder of XTend.online (unaffiliated with us).

The reasonable question was: "What should chipmakers do to not be labeled bad actors after designing a crypto (here: PoW) chip?"

We quote Chris Ziolkowski of XTend.online (unaffiliated with us but we love his answer) for our reasonable answer: "Commit to the cause of making equipment that is ubiquitous and available to anyone on an egalitarian and non preferential basis. Accept competition from others in finding the best way to secure the network. Be patient."

. . .

However we also liked Alexey's open-minded claim format so much, we take the liberty to add another set of 4 claims on top of his. If you believe Alexey's claims to be untrue, the next 4 might be even harder to

prove. If you believe Alexey's claims are true, they may be easier. Let us know.

## Claim 1: A change in PoW algorithm, or other reward algorithms in the future, must be preset to a fixed date at least 1, better 2 years in advance.

The highest principle in reward algorithms must be enabling competition.

Free and fair competition is an extension of open-source principles into hardware. Hardware requires capital and time. This means software developers have a responsibility to commit to a fixed date for the rollout of any reward algorithm in advance, long enough to enable anyone who wants to to prepare.

Equality of opportunity must be achieved. For simple hardware, 6 months or 12 months may be enough. Even for the most complicated hardware, 2 years should suffice.

## Claim 2: Open-source principles, although universally loved in crypto, do not apply to hardware.

Open does not mean open and honest. Open cannot extend well to schedules and wallets. Business negotiations and contracts are not open in many cases. One of the founding principles of open-source was that there is a mandate for code to be open, because it can be open. A bowl of spaghetti however, can only be eaten once.

The hardware world cannot make this any easier for open-source software developers. We cannot wait until the whole world becomes an open-source program. Software developers have to accept that open-source is a concept that is inherently intangible, and need to make the extra effort to define what exactly they want from the tangible hardware world.

## Claim 3: For crypto to succeed, bridging the hardware-software gap is critical.

We don't want crypto to be confined to a world of papers and github commits. PoW was a key innovation to connect the world of software

with the world of energy and time. Hardware wallets, gas turbos, accelerators for signing, proving, verifying, sorting and other things are on the horizon. Environmental impact is real, safe and fair working conditions are real. The hardware-software divide is a big challenge, but also one of the biggest opportunities in crypto in the near future. We don't believe this problem will go away with the promised switch to PoS or even an entire retreat from all things physical. Open hardware projects like Qi Hardware may help.

## Claim 4: Contributing to the network must be more economic than attacking the network.

Many of the problems we have with today's PoW come from bad alignment of incentives. It shouldn't matter that much whether all participants share the exact same goals and values, and whether their investment horizons are short-term or long-term. Protocol developers have a lot of power in structuring the rewards — issuance, monetary policy, fees. There must be no way to capitalize on inefficiencies. Devs need to understand the very real physical consequences of their economic models. Linzhi believes in a future of Proof-of-Contribution: Crypto projects will reward contribution to the actual scaling of the network: verifying transactions, STARK provers, signing, sorting, block speed, etc.

Contributing to the network has to be more economic than attacking the network. That's the principle software developers have to bring to life with algorithms and protocols, so hardware and software can grow together and in harmony.

. . .

Never stop learning.

Linzhi Shenzhen

Telegram: <https://t.me/LinzhiCorp>

# My take on ProgPOW — looking for a reasonable answer to a reasonable question



Alexey Akhunov  
Feb 3 · 4 min read

Although it may look from the post that I am “anti-ProgPOW”, I am actually reasonably neutral — so please no pitchforks. The point of this article is my discovery that being neutral might not be an option as it makes me very uncomfortable.

I have been delaying writing this opinion piece to avoid the distraction. I have just come back from the Stanford Blockchain conference. It was the first time I have attended a blockchain conference which is not specific to Ethereum (in the past I only attended Devcon, Edcon, and DappCon), and it is there that I got some insights that I was missing earlier. If you read (or just scroll) to the end, you will see what finally triggered me to write this. I reserve the right to change my opinions, and urge others not just take my word for it — use this only as a guidance and do your own research.

I will structure this opinion piece as a series of four claims. Any of them could be subjective or untrue, but I currently believe that they hold.

## Claim 1: The only ways to stop the development of specialised mining devices for Ethereum are to make ETH really cheap, or to drastically reduce mining reward

Both of these action lead to the reduction of mining revenue. Nothing else will credibly stop people from trying to develop better devices.


















Some people claim that the reason that the reason EtHash specialised mining devices appeared only recently (3+ years after the launch of Ethereum) is due to EtHash’s excellent “ASIC-resistance”, compared to other algorithms. I believe that instead this 3 years delay is mostly due to:

1. Ethereum not being worth much until the beginning of 2017
2. Credibility of Proof Of Stake replacing PoW “soon”. The key word here is “replacing”. Eth 2.0 pivot in June 2018 meant that PoS and PoW chains will coexist, at least for some time.

It appears to me that the growing consensus among blockchain developers is that it is counterproductive to fight the specialisation of mining hardware. The goal instead should be indirectly fostering (or at least not resisting) more competition in the mining hardware development, which can be achieved by keeping mining “rewarding”. This can be done either by increasing the rewards, or by decreasing the mining costs. Both EIP-1234 (reduction of reward) and ProgPOW (increase of mining cost) go into the opposite direction.

## Claim 2: GPU mining is a losing battle, and Ethereum is the last bastion

If we look at a very helpful table of how much miners earn per day in USD, from messari.io, and recall that Bitcoin, Dash, Litecoin, ZCash, Bitcoin Cash are predominantly mined with specialised (not GPUs) hardware, it becomes clear that Ethereum is “the last bastion” of GPU mining.

Name	New Issuance (24hr, USD) ▼	Fees (24hr, USD)
 <b>Bitcoin (BTC)</b>	\$6,664,494.21	\$99,877.20
 <b>Dash (DASH)</b>	\$523,940.57	\$145.47
 <b>Litecoin (LTC)</b>	\$456,194.69	\$437.60
 <b>ZCash (ZEC)</b>	\$338,219.16	\$71.72
 <b>Ethereum (ETH)</b>	\$270,942.53	\$5,731.39
 <b>Bitcoin Cash (BCH)</b>	\$211,597.73	\$49.29
 <b>Decred (DCR)</b>	\$80,824.93	\$30.51
 <b>Digibyte (DGB)</b>	\$35,806.83	\$0.444
 <b>Dogecoin (DOGE)</b>	\$26,453.35	\$102.29
 <b>Monero (XMR)</b>	\$19,854.99	\$22.41
 <b>Bitcoin Gold (BTG)</b>	\$18,471.18	\$3.31
 <b>Ethereum Classic (ETC)</b>	\$18,046.04	\$8.58
 <b>Verge (XVG)</b>	\$11,103.78	\$3.83
 <b>PIVX (PIVX)</b>	\$6,720.03	\$20.20
 <b>Vertcoin (VTC)</b>	\$3,483.94	\$0.215
 <b>XRP (XRP)</b>	no data	\$67.46
 <b>Stellar Lumens (XLM)</b>	no data	\$0.323

I do not anticipate any new cryptocurrencies launching with the aspiration of being “ASIC-resistant”. Notable example is Grin, which will increase the reward share of their ASIC-friendly algorithm from 10% to 100% within the first 2 years after launch. Decision of Grin to actually make one of the algorithms ASIC-friendly is due to their hope that making ASIC design simpler will encourage competition. Here is the relevant video link.

## Claim 3: Hardware design shops are getting better at what they do

One of the most interesting takeaways from David Vorick’s talk (video link) for me was that the process of designing digital chips is separate from “taping out”, which is in turn separate from the actual fabrication. Another interesting fact about people like David is that it does not take a very long time (1–2 years) for a very good software developer to learn enough about hardware design to set up a design shop. The required information to do such a transition is not well shared and accessible, so

one has to learn directly from people, but such transition is not at all impossible. Hardware design is not a black magic and I expect, given the demand, the number of independent hardware design shops will only grow.

## Claim 4: Pursuit of “ASIC resistance” is a strategy of denial that can hurt more than help

There were some calls to the Ethereum protocol developers to come up with the “Guidelines for the developers of the specialised mining hardware for ProgPOW on Ethereum”. At first, I did not really understand what these guidelines would be. But recently someone has explained to me that it would be basically answer to the question: “Hey, Ethereum protocol developers, we heard you are switching PoW to ProgPoW. We want to start designing a specialised hardware for it (yes, we know that you think we shouldn’t, but it is neither illegal nor unethical to do it, so we will give it a shot). Please tell us what we should do to make sure we are not labeled as bad actors after the fact”.

This is a very reasonable question. But if you subscribe to the ASIC-resistance strategy, the only answer you can give is this: “There is nothing you can do to prevent being labeled as a bad actor. We don’t want you to develop your hardware, and if we see that you have succeeded, we will try to do another PoW change so you cannot sell your hardware and go out of business”. Which is not a very reasonable answer, and can hurt more than help.

This combination of reasonable question and unreasonable answer is what actually motivated me the most to write this article in the first place. So what the reasonable answer should be?