Linzhi Semiconductors

Linzhi Working Papers
No 5

Linzhi Telegram January 7 to 29, 2019. Lessons Learned.

by Sonia Chen

January 2019

Keywords: LWP5, Telegram, ProgPoW, Debate, Ethereum

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

Our Telegram, January 7 to 29, 2019 — Lessons Learned

Linzhi ASICs
Feb 1 · 7 min read

On January 8, 2019, Linzhi Ltd, a private fabless semiconductor company in Shenzhen, called upon Ethereum developers to publish rules and guidelines for what constitutes a good ProgPoW ASIC maker.

https://www.coindesk.com/ethereum-miner-linzhi-calls-out-project-coders-for-proposed-asic-ban

Little did we know that an intensive debate between many stakeholders would ensue, and since we now feel that has come to a conclusion, we want to summarize lessons learned, our takeaway. Biased.

. . .

Ethereum Governance

Ethereum is a wonderful project, decentralized, romantic. Anyone can be a developer, pseudonymous and anonymous members are welcome. Motives or second agendas are not questioned in crypto utopia. Polkadot, cat herders, magicians, Vitalik, core devs, Ethereans, ProgPOW, classicists. We are all Ethereum.

. . .

ProgPOW

When we first read “technical papers” from ProgPOW supporters that didn’t add up, we knew something was different, but just what?
Today we know that ProgPOW follows the energists philosophy (more later), in line with their affiliates and business practices we have seen from Coingeek, Craig Wright, nChain, etc. There may be truth in this approach, but it’s not our truth.

We think ProgPOW is a bad idea not only because of motives and who will win or loose, but because the following values will be impaired:

- Technical Excellence: ASIC resistance not much different from Ethash.
- Equality: Chinese miners will be bricked, creating waste.
- Environmental Responsibility: Power consumption of ETH network seems to be going up, there is limited data on the subject.
- Open Source: Open source audit cannot see power consumption, cannot see which existing chips favored, cannot see how hard or easy to design new chips.
- Community Consensus: Process of PoW change in general (for any coin not just Ethereum) is not thought through, many problems are not identified or understood.
- Decentralization: Verification slowed by unknown factor, asymmetry between proof and verification helps decentralization.

. . .

Lipstick on a Pig

Aside from copious proofs of dirty backroom deals, we got some amazing anti-ProgPOW artworks from the community. Our favorite is this poem. Noone can make this up, thank you Anonymous!

> *The ProgPOW initiative is teaching us to return to incandescent light bulbs. There's no reason to improve energy efficiency beyond what GPU technology provides.*

> *The ProgPOW initiative is teaching us there's no reason to spend time advancing crypto mining technology. GPUs are as good as we're allowed to have.*

> *The ProgPOW initiative is teaching us that GPUs are god, and the GPU god sets the rules, and the GPU god favors his acolytes. Officers and investors in a mine who are heavily invested in GPU equipment and have insider*

> *connections to the GPU god plus influence in the Ethereum core development team write a protocol that favors their mine revenues and GPU makers.*

> *The ProgPOW initiative is teaching us about arrogance. Those revolutionary advances in memory technology and semiconductor fabrication now heading for commercialization belong to the GPU god. Shh! Don't tell them that those advances are going to render PropPOW worthless in a few years.*

> *The ProgPOW initiative is teaching us that open source doesn't mean full transparency. Who originally developed and wrote the protocol? Who underwrote the original effort? Who's been promised some future benefits? Did those involved fully disclose their self-interests? And what's the real motive for this initiative?*

> *The ProgPOW initiative is teaching us how socialism really works. Anyone who attempts to excel at mining is penalized until everyone mines with equally poor performance. Individual rights are subjugated to the crypto-state controlled by the privileged few.*

> *The ProgPOW initiative is teaching us about hypocrisy. The developers of ProgPOW proclaim the socialist mantra of "fairness" while using the "fairness" algorithm to neuter potential competition that threatens their capitalist enterprises.*

> *The ProgPOW initiative is teaching us again how the "fairness" mantra appeals to the masses whose educations didn't include a history of the "fairness" movement. Only later do they discover that the price was their freedom. In this case, that freedom was to mine and otherwise prosper but those rights are now subjugated to the crypto-state controlled by the privileged few. Perhaps, advocates should consider the millions of people protesting and fleeing Venezuela to find freedom.*

> *The ProgPOW initiative is teaching us a socialist subjugation tactic — spread "fairness" to neighboring crypto-currencies just in case you think*

> *about fleeing.*

> *The ProgPOW initiative is teaching us an ugly anti-competitiveness tactic — secure adoption while the protocol specification remains a bit fluid and hint that further adjustments may be necessary. Is the intent to permanently discourage FPGA and ASIC development efforts? And who determines when adjustments are needed? The GPU god? An anointed acolyte?*

> *The ProgPOW initiative is teaching us how to foster a legal quagmire for monopolistic restraint of trade practices that invite government intervention.*

> *The ProgPOW initiative is teaching us to wonder why members of the core development team have not raised the issues above. Is this how they want to be remembered when the history of Ethereum is written? And that history may be much briefer because of the issues above.*

> *The ProgPOW initiative is teaching me to look for another blockchain platform for a major program.*

> *Anonymous*

. . .

Chipmaker Social Contract

It looks like manufacturer-neutral open hardware forums might pick this up (see Qi below), but the essence of our ideas for chipmaker guidelines to enable competition in the crypto era are (thanks to many who contributed):

- cost transparency
- production transparency
- sell to developers and community first

- volume discounts topped out at fixed percentage
- recycling program, protection against loss of value, bricking
- no self-mining, sell to independent customers only
- transparency in developer relations and funding
- qualifying customers, no sales to ponzi, mlm, scammers, etc.

. . .

ASIC Resistance

.. is a state of mind. MoneroCrusher's article and our response remain our memory.

https://medium.com/@MoneroCrusher/opinion-asic-resistance-is-a-state-of-mind-not-something-you-can-achieve-with-a-final-software-abdc878a50aa

https://medium.com/@Linzhi/its-the-unknown-we-fear-response-to-monerocrusher-f7885bea5983

. . .

Open Source

.. is the over-arching value guideline. Unfortunately proven open source principles reach limits when dealing with energy and time. No amount of code study will tell you much about power consumption, business motives, hardware costs, etc.
We hope the discourse of how to extend open source principles into hardware will be continued. Open source principles are great!

. . .

Hobby Mining

.. is the desire of many, and we have too few answers for that. Mining needs to be FUN again. Mining should be possible with a 200 USD investment, with hardware that can easily be bought, and if mining

doesn't work out, can be sold again. Even with an unsellable GPU card you can still play Fortnite!

. . .

GPUs for PoW

.. are a bad idea in the long run. PoW is a cryptographically and thermodynamically provable security mechanism. To understand why GPUs are a PoW dinosaur to mainly benefit Nvidia/AMD insiders and large farms, we propose reading Chris Ziomkowski's wonderful article.
https://blog.usejournal.com/inside-the-new-crypto-mining-technology-that-will-redefine-the-industry-196529547c88

In our view it's not ASICs that lead to centralization, it's cost advantage.
https://medium.com/@Linzhi/asics-and-51-achieving-mining-dominance-how-cost-advantage-drives-centralisation-cf28166d3d2a

A major reason the computing industry evolved around the Von Neumann architecture is that it is easy to develop software for. The instruction set is intuitive for humans to understand.

Imagine how difficult it would be to compile an algorithm to Conway's Game of Life hardware.
https://en.wikipedia.org/wiki/Conway%27s_Game_of_Life

There are thousands of computer architectures in history. The Von Neumann bottleneck does not apply to other computer architectures. Most of them never succeeded commercially although it is not difficult to actually build that hardware. Without a language, compiler, debugger or development method, these kinds of hardware can never be accepted by the industry.
Mining is a different market. Mining hardware mostly sells its service directly to the network, instead of selling to people who need to do development for the hardware. The network will reward the correct result automatically, but it cannot verify which implementation is providing the result. You could use paper and pencil to mine Bitcoin.

This opens the possibility of selling special hardware without programming language and development methods. Implementing one

algorithm on special hardware is easy, but creating a toolchain or design method is much more difficult.

ProgPOW is still one algorithm, even if it has a pseudo-random sequence inside, it's still a single algorithm.
ProgPOW's parameters are optimized for a GPU, assuming the performance upper bound is limited by memory bandwidth, and the cost lower bound limited by (pseudo-random) logic requirements.
It will prove GPU limits, but will never prove that ASICs need to use the same implementation.

. . .

Upcoming Ethash Miner

.. is on track, maybe with a small delay, but we enjoy working on this chip and bringing more security to the ETC network and anyone else who wants Ethash security.

. . .

Proof of Contribution

.. is our vision for the way forward. Making contributing to the network more economic than attacking it. Making chips not just for PoW, but for signing, verifying, proving, sorting, block speed, other things. The biggest obstacle for any forecastable chip demand is lack of user adoption. Self-referential mining games with ever more sophisticated insider plays will end.
Our attention will go to hardware that enables financial liberty, user adoption.

. . .

Energists

ENERGISTS will always get energy as fast and efficiently as possible. #1 rule of ENERGISTS is to get energy for self. Golden Rule and other rules of humankind are thrown out or used in service of the needs of ENERGY gathering.

That is why the words do not add up if you use the old ways of pre-crypto thinking.
If you want to understand the ENERGIST, you must think like the ENERGIST.
Better to think like a plant or a tree, then the words will make sense…

Thanks to Jon Phillips.

. . .

Qi Hardware

Jon proposed Qi Hardware as a forum for open hardware collaboration, we will try to contribute as much as we can.
https://qihardware.org/
Open source (MIT/GPL) code and documentation for Linzhi chips will be published at https://github.com/LinzhiChips (there is nothing yet).

. . .

That was a fun month of January for us, thanks a lot to everyone who contributed and we hope others learned many things as well.

Never stop learning.
Linzhi Shenzhen
Telegram: https://t.me/LinzhiCorp