Linzhi Semiconductors

Linzhi Working Papers
No 4

Responding: ASIC Resistance is a State of Mind.

by Sonia Chen

January 2019

Keywords: LWP4, ASIC Resistance, Fear, Ethereum

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

Linzhi ASICs
Jan 15 · 7 min read

It’s The Unknown We Fear: Response to MoneroCrusher

Once in a while when reading articles, you come across the one you feel is different. A like-minded soul searching for something? Or maybe not? You are willing to investigate…

ASIC resistance is a state of mind, not something you can achieve with a final software implementation.

MC: There will always be a specialized device that is going to beat the big decentralized GPU mining community.

Yes.

MC: The more efficient machine will always replace the less efficient one.

Yes.

MC: The current ASIC market weakens the security, integrity and decentralization of PoW based cryptocurrencies.

We believe the opposite. Our customers agree and never brought up this subject. You say “current” market, there is hope to change what bothers you. The market is a result of our work.

MC: All GPUs are an assembly of ASICs themselves.

Yes.

MC: The EF & the Ethereum Core Developers risk tainting their image permanently.

This should be our top concern, second being environmental impact.

MC: This is literally a billion dollar business.

It is, and unlike free software source code, business considerations are by default (though not necessarily so) intransparent. The current intransparency of this business is where we believe is a chance for improvement. Not just on the software side — transparency on the software side is pretty good.

MC: PoW & ASIC-resistance: If you want it, you have to fight for it — play the game!

Again?

MC: General purpose. Adapting to various chaotic and changing circumstances with little effort.

All hardware is the same. New ASICs are better at adapting to chaos than GPUs, because GPUs are stuck technically and economically in a fixed architecture. This is a key point from our view.

MC: Monero hasn’t seen a large ASIC takeover of the network since its first anti-ASIC fork.

You probably mean a “non-Nvidia, non-AMD” takeover. That seems to not have happened yet.

MC: ASICs on the Monero network.

You mean non-Nvidia, non-AMD.

MC: … they have just become smarter about it and made it less obvious

Sounds like a sad story.

MC: Ethash has proven itself to be extremely good at keeping ASIC efficiency gains pretty close to a GPU’s efficiency.

It wasn’t worth yet to make better ASICs. The Bitmain, Innosilicon etc. ASICs are already beating GPUs easily. If you already win the race, you don’t need to spend more money to make your race car faster.

MC: Efficiency gains much smaller with Ethash.

Efficiency gains are more expensive with Ethash. Cost is the only difference.

MC: Takeover of the network would cost hundreds of millions in funds

We think it’s much less, but our customers take that risk. We see strong demand for PoW asics, of any algorithm, from small home miners to mega farms (100MW+).

MC: Risk is immensely increased for ASIC manufacturers and their investors.

Risk is increased for our customers, not us. Unless you believe you can destroy PoW altogether, then the risk is for us as well and we need to focus on non-PoW chips.

MC: Carbon footprint will also be kept lower.

We should talk about this more, it should be one of our highest organising principles. The original ASIC-Resistance thoughts from the 2014 Yellow Paper ought to be brought forward to reflect what we learned in the last 5 years. ASICs use less energy. You don’t resist ASICs because they are less energy efficient? We think the reason for ASIC-Resistance was that people thought they lead to centralisation. We think that’s a fundamental misunderstanding: The cause of centralisation is cost. ASICs reduce the energy requirement of the network prior to PoS.

MC: Say currently set 1 (Ethash) consumes 1 GW of power, set 2 (ProgPOW) would increase it to 1.3 GW of power.

If your numbers are true, that alone should make us reject ProgPOW. What world are we in in 2019 that we can afford to waste 300 MW of constant load for …. for what? Can a large farm help the community with solid numbers? This is important!

MC: solution … fork … unpredictably every 6 months

Will reward secrecy.

MC: GPU miners don’t have to worry about anything.

It was wrong in the past, it stays wrong in the future. GPUs are a good tool to start a network, and for development. For large systems, GPUs can’t maintain their cost/efficiency/performance advantage.

MC: Equivalence of 30% of the maximum output of the Clinton Nuclear Power plant.

We think 75% of mining uses green energy, and may actually be consuming excess capacity on the grid, and even supporting the profitability and as a consequence the development of renewable energy generation capacity. It may be net beneficial for the renewables space, but more research is needed in this area.

MC: Opposing arguments to this could be: “the more energy is expended, the more secure the network becomes”.

We believe security comes from the asymmetry between hash and verification. Hashing is hard, and thermodynamically provable hard, while verification is easy. Ease-of-verification is an important decentralising force, unfortunately also hard to quantify.
The argument of expending more energy to make the network more secure must be rejected.

MC: If you want Proof of Work to work in an originally intended decentralized fashion.

We also believe efficient decentralization is the main goal, and free competition between asicmakers (including GPU) is the best way to reach it.

MC: You’ve got to put work in (pun intended).

We always loved the work part in Proof-of-Work. Hardware is hard.

MC: AMD always allowed VBIOS modding on their cards

Yes.

MC: Nvidia cards have much better alternatives if mining dies down: > reselling or repurposing for HPC/DL/ML.

Yes. Important to think about these things. Waste reduction is important.
Frivolous bricking of miners is littering.

MC: What ProgPow factually does … They want to have the benefits of low risk and at the same time the rewards of high risk.

Common sense tells us there are probably reasons for that.

MC: Mining centralization and ASICs will ultimately cripple the decision-making process of the currently independent Ethereum Foundation and ETH Core Developers.

Our proposal is:

1. Actively govern the competition of multiple asicmakers (including GPUs) with each other.
2. Announce PoW algorithm changes a long time in advance (we proposed 2 years), to remove most incentives for special interests to influence the EF/devs. The longer you announce in advance, the less incentive there is. The shorter you announce in advance, the more you reward the wrong thing.

Just because we are asicmakers doesn’t mean all of our ideas are bad. We see some problems earlier than others, and some later than others. That’s where dialogue starts. Maybe asicmakers do not have to be bad and can be governed just like anything else.

MC: Signal to community that ASIC resistance is a goal and that it is a current problem.

ASIC resistance is the problem. The solution is ASIC friendliness.

MC: If evidence arrives of massive ASIC takeover.

You are calling for asicmakers to self-mine and do secret deals with large farms.

MC: That’s the ultimate step towards psychological warfare on ASIC manufacturers

We are already here.

MC: and their respective investors

The asic investors care about whether there are enough paying customers. asicmakers care about the future of PoW.

MC: Only here to suck out every last drop of everything that makes cryptocurrency such an amazing concept.

We think we are equal.

MC: (that being mainly decentralization).

ASICs don’t lead to centralization, cost advantage does.

MC: ASIC manufacturers are not expected, nor incentivized to truly change their practices anytime soon, if ever.

Step up and demand change. We are in Shenzhen, we can translate all documents bilingual. We can create global rules, communicated in English and Chinese, for a healthy PoW system, with focus on good governance, environmental impact, waste reduction. In the case of Ethereum, maybe only until PoS arrives. In the case of others, maybe longer. But the “it’s only for a little while until PoS arrives” argument shouldn’t mean that we do a lousy job until that day. We believe the following list is a good first set of guidelines for PoW asicmakers:

1. cost transparency
2. production transparency
3. sell to developers and community first
4. volume discounts topped out at 20%
5. recycling, protection against loss of value
6. self-mining only when unable to sell and fully transparent
7. transparency in developer relations and funding
8. qualify customers, no sales to ponzi, MLM, etc.

MoneroCrusher and Linzhi can work together on this. We have to overcome stereotypes, but today can be the day we start. If someone tells us it can’t be done, we know it can. We are ready.

MC: brick current fixed function hardware aka ASICs

Bricking miners is littering.

MC: minus the ASIC manufacturers, but nobody cares about those

Why not?

MC: they knew what they had signed up for when they secretly created ASICs

We focus on our customers. As long as they are happy, we are happy.

MC: A project that states an anti-ASIC stance in its founding document, the Whitepaper.

We believe it’s unfair to hold authors of a document written in 2013/2014 accountable for every last word in every paragraph forever, and in a fast-changing high-tech environment in particular! The development and realizations of the past 5 years could not have been predicted by anyone. Never stop learning.

MC: Chaos and ASICs are like oil and water — they just don’t mix.

We love Approximate Computing.

. . .

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

Opinion: ASIC resistance is a state of mind, not something you can achieve with a final software implementation

MoneroCrusher
Jan 15 · 13 min read

Dear Community,

After intensively looking at, keeping up with, participating in and promoting several ways to achieve ASIC resistance for over a year I finally came to a conclusion for myself, which I am going to walk you through in this article.

I was once one of the earliest and biggest supporters of ProgPow (end of April/start May 18) and have from the very beginning endlessly rallied for it because I firmly believed it will bring final and definitive ASIC resistance to Ethereum (or a maximum 20% stated speedup for a specialized implementation), even though my first instinct when I saw it was that it's going to disfavour me as an AMD Polaris card owner in comparison to other architectures in relation to Ethash. But I was happy with it because I just wanted ASICs to be gone. I have also closely followed other solutions like RandomJS, RandomX, Rainforest and MTP.

All seemed intriguing at first but eventually it dawned upon me: no matter how hard you try, there will always be a specialized device that is going to beat the big decentralized GPU mining community, because if there's a possibility to get an edge over others, there will always be someone that has the means, the will and that's going to try and get it and eventually achieve it.

Notice how the goalpost has recently been moved in the ProgPow talks. As of late in various chats and groups I see claims from a multitude of people that speedups of more than 50% are possible with ASICs and even IfDefElse have adjusted their Medium post adjusting ASIC efficiency gain to 50% (Linzhi claiming even much more, unproven) and the discussion is revolving a lot about designing them and I'm sure somebody will figure out a way eventually and secretly use it to their advantage. How is that better again vs. an ASIC that has a 100–200% speedup in Ethash? It's in the same ballpark. If there's a significant efficiency gain, the more efficient machine will always replace the less efficient one, Economics 101.

Don't get me wrong here, as a GPU miner I'm still 100% in the firm believe that the current ASIC market weakens the security, integrity and decentralization of PoW based cryptocurrencies.

But there has to be a different approach to it:

STOP TREATING A PROOF OF WORK ALGORITHM AS A HOLY GRAIL — SOMETHING IMMUTABLE

You don't download the latest Linux Kernel and expect to never have to upgrade it again in your whole lifetime, right? There are going to be bugs and weaknesses detected, and they get patched with the flow of time. If you've got ASIC resistance in mind — and see ASICs as a weakness in a network's security, integrity and decentralization — then treat it as such.

There's never going to be a final one-time software fix to kill all ASICs — it's a Fata Morgana, the last little straw held on tightly by the highly desperate GPU miner community — including, for a long time, myself. All GPUs, by their very technical definition are an assembly of ASICs themselves. It's always going to be a cat-and-mouse game. Like it has always been in the soft-& hardware industry and for that matter, in virtually every other aspect of life (think of bacteria and anti bacteria medication).

With regards to forking to a "one time solution to kill all ASICs", the EF & the Ethereum Core Developers risk tainting their image permanently by favouring one manufacturer over the other (for example ProgPow factually shifts the power dynamics between AMD and Nvidia by A LOT, *if you take Ethash as the base*), as it can never be ultimately proven that an author of a radical (emphasis) and newly proposed algorithm doesn't have big funding or other incentives behind them (hint: the EF/Ethereum Developers will *always* make the "wrong" decision no matter what they choose to do — if they enter that arena). In the case of ProgPow, I personally believe many conflicts of interest to be involved, but I'm not trying to make that the topic of discussion in this article, because with such radical changes — ProgPow is one — there will always be different interests pushing either one or the other agenda, this is literally a billion dollar business. Imagine.

But I do have a solution in mind that will satisfy and represent the majority of the current Ethereum Ecosystem, while also to the best possible extent reintroduces decentralization of hashpower. I am going to suggest that the EF, the Ethereum Core Developers and the Ethereum community should change their state of mind with regards to PoW & ASIC-resistance: If you want it, you have to fight for it — play the game!

Instead of trying to chase the pink dragon, ask yourself what general purpose hardware is best at? Yes, you guessed correctly: General purpose. Adapting to various chaotic and unpredictable changing circumstances with little effort.

Monero has taken on the same approach and it has more or less been a successful one, it hasn't seen a large ASIC takeover of the network since its first anti-ASIC fork, however, I strongly believe that there are ASICs on the Monero network at this very moment, they have just become smarter about it and made it less obvious to detect by reducing their quantities, deployment strategies and risk (the manufacturers).

The reason and much higher likelihood of it still happening on Monero is because the efficiency gains with an ASIC on Cryptonight are extreme (we're talking about a 50–100x speedup), that's why they are still brought into the light of the day — in secret. With Ethereum it's a whole other story. Ethash has proven itself to be extemely good at keeping ASIC efficiency gains pretty close to a GPU's efficiency (we're talking about a 100–200% speedup (Linzhi claims 800% that we have yet to see)) vs. other algos losing to ASICs sometimes dozens, hundreds or even a thousand time more efficient than a GPU.

Taking on an active approach will help keeping ASICs to a minimum, better so than any PoW algorithm claiming to do so ever could (e.g. ProgPow or insert X here) and it will never happen again on the large

scale we see today until PoS is finally implemented or cryptocurrency sees a dozenfold increase in price until that happens (i.e. reducing manufacturer's risk). Why will it work on Ethereum? Because the network is huge and efficiency gains much smaller with Ethash. A repeated big takeover of the network would cost hundreds of millions in funds, and they'd only have 180 days to break even, forget make any money — in this market: absolutely impossible. But I believe there will maybe be smaller batches of ASICs within those 6 months by talented, small and flexible companies, but it will never be nearly as bad as it is today, because by taking on this new stance, risk is immensely increased for ASIC manufacturers and their investors — but please just accept the fact that they're undoubtedly inevitable as proven many times on various algorithms in the past.

Energy Consumption

As a neat side-effect of forking every 6 months, the carbon footprint will also be kept lower than changing to a more power hungry algo that claims to minimize ASICs:

Imagine all GPUs on the Ethereum network (and it solely consisting of GPUs). Once as "set 1" and once as "set 2".

Say currently set 1 (Ethash) consumes 1 GW of power (which based on my estimates is pretty close to reality) and set 2 (i.e. ProgPow) would increase it to 1.6 GW of power at any given time, assuming a very conservative additional power draw and increased cost of cooling (and assuming most farms will just increase air throughput at low cost).

One solution is to to keep Ethash and fork the PoW minimally, but significantly and unpredictably every 6 months. GPU miners don't have to worry about anything, while ASIC makers will always be on their toes, trying to anticipate the next change if they choose to play the game. Even if they succeed in anticipating it, they only have 6 months until the next fork, which will render their hardware useless. With solution one economies of scale start to *crumble.*

In this case the power consumption is kept at 1 GW.

The other solution is to take e.g. ProgPow that uses more of a GPU, and therefore makes it harder for ASICs to gain as much efficiency as before. In solution 2 you will increase the power consumption to 1.6

GW, while ASICs eventually will come back anyway with their economies of scale, which work perfectly fine with ProgPow.

With solution 1 about 600 MW of power at current crypto market prices (implying more or less hardware getting deployed to the network) is saved, which is the equivalence of 60% of the maximum output of the Clinton Nuclear Power plant while also getting better ASIC resistance than with solution 2.

Clinton Nuclear Power Plant — Maximum Output: 1062 MW

Opposing arguments to this could be: “the more energy is expended, the more secure the network becomes”, that is largerly true but in this case we have the same amount of GPUs in “set 1” and “set 2” and therefore it seems far-fetched that it decreases network security from a computational standpoint at all. Memory is much more expensive than compute, and Ethash strongly features the former, meaning GPUs are already pretty damn optimized for Ethash, and there won’t be a government or corporate takeover with an alien hardware, as has been proven in the past 5 years. So given that we only have GPUs securing the network anyway (with this new policy), and given that “set 1” and “set 2” feature the same array of GPUs, we can conclude that by using more power on “set 2”, it doesn’t make the network more secure (marginally, if at all), but only linearly more wasteful.

Following the last conclusion I can make the following statement: Ethash with a 6 month fork cycle is 37.5% more energy efficient at securing the network with a fixed set of GPUs than ProgPow.

The only drawback in solution 1 is that it has to be maintained by the devs and the miner community. It has worked out pretty well in the Monero community, all sorts of changes coming in all over the place from all kinds of people, publicly reviewable on Github and each fork is mostly highly anticipated by miners because of increased profits — I would claim the Monero devs and Monero miners are in a very harmonious relationship, even more so because of their anti-ASIC actions as of late. The October fork was so smooth, it was barely noticeable that it ever even happened. An example on how to do it well: CNv3 is currently in development and if it passes review, all a miner has to do is update the software and start mining again, I personally tested it and I didn't have to adjust clocks or voltages by a single Mhz/mV to achieve the same hashrate.

But I have a point to make with regards to developer effort as well:

A 6 month fork cycle will generate its own dynamics and a "movement". It incenvitizes more people, especially from the miner community to actively help find fair solutions for the next fork, this can then be reviewed and tested by anyone. Ethereum miner developers are also incentivized to write better code because there's more on the table for them, once the ASICs are gone. Therefore it will not put all the burden on ETH Core Devs and doesn't deviate them from their long-term roadmap goals, but a separate additional "fork-community" will form, as it did in Monero. Just check out user sech1's reddit flair: "XMR contributor — ASIC bricker", isn't that badass?

But as I said, if you want Proof of Work to work in an originally intended decentralized fashion, you've got to put work in (pun intended). As everywhere else in life, you can't just come up with a solution once and expect it to work forever.

Decentralization, why it's important and why ProgPow and other one time solution attempts that concentrate on increased GPU usage will worsen it (even if they mean it well):

First of all, the major and most used cards on the Ethereum network used by the Average Joe (and also overall) are AMD Polaris cards.

Reason being because AMD always allowed VBIOS modding on their cards and therefore was able to offer the Ethash mining market the best hash/dollar and hash/watt ratio and was — at least for the large public — the most efficient device to get for, to mine Ethereum with. To clarify this a little better: private people and private companies all over the world that had the sole goal of mining memory hard based algorithms like ethash and wanted the most efficient device for it, got themselves an AMD Polaris card. While on the other hand, entities wanting to enter the mining space, but at the same time wanted to minimize their risk exposure went for Nvidia cards. Reason being because Nvidia cards have much better alternatives if mining dies down: reselling or repurposing for HPC/DL/ML. We can categorize the Nvidia part of the network “lower risk/lower reward” and the AMD part “higher risk/higher reward”.

What ProgPow factually does, is take hundreds of millions worth of investment out the the majority of the Ethereum network (AMD Polaris infrastructure owners), and puts the delta 1:1 ontop of Nvidia datacenter owners. They want to have the benefits of low risk and at the same time the rewards of high risk. In other words: “They want to have the cake & eat it too.”

Additionally ProgPow will only deepen the crater between hobbyist miners and megafarms. We all have to admit that there will never be perfect decentralization because of geographical differences and associated costs of running a farm, but what we can do is to soften the blow the best we can. But by adopting ProgPow and it consuming a lot more electricity than current Ethash, the hashpower further shifts to the megafarms with cheap power available and I bet that if any ProgPow ASIC ever would get created, it would also concentrate mostly in their hands because of special relationships and economies of scale.

Furthermore I strongly argue that mining centralization and ASICs will ultimately (try to) cripple the decision-making process of the currently independent Ethereum Foundation and ETH Core Developers. As it so often happens in centralized governmental structures, where the centralized structure eventually gains so much leverage and power, that they virtually control every part of a nation and the overall life-quality of its people, while benefitting themselves the most. Therefore it’s important to distribute the power and keep it that way as good as possible. So let’s try to not turn everything into banking or central banking — crypto special version.

We are a grassroots movement, so let's PLEASE not repeat the mistakes of the past.

The steps forward:

1. Signal to community that ASIC resistance is a goal and that it is a current problem
2. In a community driven effort find a small tweak to implement in Ethash_v0
3. Review ethash_v1 and run on testnet
4. Fork it!

Additionally:

1. Separate fork schedule HFs and mainline schedule HFs. Additionally state "We reserve the right to apply emergency PoW forks during the mainline forks as well, if evidence arrives of massive ASIC takeover and/or in case a critical weakness in the PoW is found". That's the ultimate step towards psychological warfare on ASIC manufacturers and their respective investors that are only here to suck out every last drop of everything that makes cryptocurrency such an amazing concept (that being mainly decentralization). ASICs are a lost cause, because they only allow for people with economies of scale available to particpate and that excludes 99.99% of the decentralized Ethereum community and

as evident in the past, ASIC manufacturers are not exptected, nor incentivized to truly change their practices anytime soon, if ever.

2. As a first change, you could for example change FNV1 to e.g. FNV1a to prevent FPGAs from exploiting the existing critical bug in Ethash (they support the instructions to do so, talked with various FPGA experts in private about it) + change something small in the algorithm and at the same time brick current fixed function hardware aka ASICs. I have not much against FPGAs generally speaking.

3. Reddit user and Ethereum Core Developer u/5chdn posted a list of other potential changes and I found https://github.com/ethereum/EIPs/blob/master/EIPS/eip-969.md to be the most interesting so far, maybe it can be reviewed more in-depth for the first small change?

If we give PoS a maximum deployment time of 2 years, then that's only 4 tweaks to Ethash until then.

I believe this is the best way of preventing a big community fallout, general ugliness and mud-throwing, because it's perfectly aligned with the way the network is currently laid out, minus the ASIC manufacturers, but nobody cares about those — they knew what they had signed up for when they secretly created ASICs on a project that states an anti-ASIC stance in its founding document, the Whitepaper. And yes, expect a ton of sometimes subtle, sometimes obvious FUD from people that will not profit from this (ASIC manufacturers and other special interests).

https://github.com/ethereum/wiki/wiki/White-Paper (Chapter: Mining Centralization)

Also: It is important to set Ethash as it currently stands as "ground 0" for all comparisons of efficiencies because the whole infrastruture that is now worth $ billions is built around it the way is currently is, because of the way it was originally designed. Unless you want to accuse Vitalik of colluding with AMD when creating Ethereum, of course.

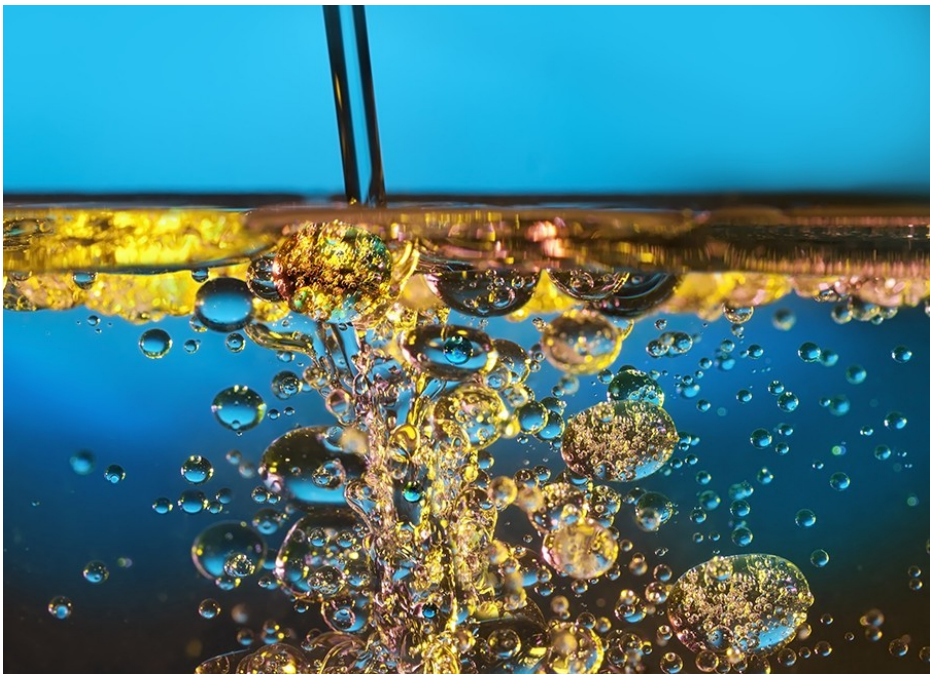
I understand that it can be frustrating for all the devs that have started implementing ProgPow into their software stacks, but more often than not, the first and most obvious solution of approaching a problem is not

always the best
https://en.wikipedia.org/wiki/Theory_of_the_second_best.

Closing remark:

Chaos and ASICs are like oil and water — they just don't mix.

(misappropriated quote by Jasper Fforde)



Sincerely,

MoneroCrusher