Linzhi Semiconductors

Linzhi Working Papers

No 15

Posts against ProgPoW - 2019 May-Sep

September 2019

Keywords: LWP15, ProgPoW, Resistance, Ethereum

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

Posts Against ProgPoW - 2019 May-Sep

This is a collection of Linzhi's debate contributions from May to September 2019, with contextual contributions by Tim Olson, OhGodAGirl (Kristy-Leigh Minehan) and others.
The purpose of this collection is to document the authenticity and validity of Linzhi's contributions, and to serve as a focal point for further investigations into ProgPoW.
The full threads on the Ethereum Magicians Forum are hard to parse because of repeated attempts to derail the conversation.

We do not attempt to provide any documentation of the pro-ProgPoW arguments, and include such posts only where necessary to provide context.
We add that we observed editing and deleting of pro-ProgPoW posts in social media, weeks or months after posts were made. We also suspect, without evidence other than eyebrow-raising continuity of some details, that several authors writing pro-ProgPoW posts under a variety of accounts are in fact all writing in a coordinated way.

This collection merges posts from both threads chronologically. The collection ends with Linzhi's last contribution on September 6, 2019.

Sources:

EIP-ProgPoW: a Programmatic Proof-of-Work (2018-05-03)
https://ethereum-magicians.org/t/progpow-audit-delay-issue/272

ProgPoW Audit Delay Issue (2019-05-23)
https://ethereum-magicians.org/t/progpow-audit-delay-issue/3309

Linzhi Team, Shenzhen, September 25, 2019
Telegram: **t.me/LinzhiCorp**

---

ifdefelse #1 January 16, 2019, 7:23am

We propose an alternate proof-of-work algorithm tuned for commodity hardware in order to close the efficiency gap available to specialized ASICs. Thanks in advance for your thoughts and comments!

EIP here: **https://github.com/ethereum/EIPs/pull/1057**
Implementation here: **https://github.com/ifdefelse/ProgPOW**

1 Like

souptacular #1 May 23, 2019, 6:04pm

Hey all! I have an important topic for discussion.

We ran into issues starting the ProgPoW audit. We had a hardware partner who specialized in ASICs who was going to work with Least Authority to perform the hardware parts of the audit. They are no longer participating in the audit so we are looking for other auditors for the hardware portion. We have some good candidates, but this effectively delays the start of the audit much more than we anticipated. Because of this I am unsure if the audit will be complete before Istanbul. On top of that I am not sure if anyone has sorted the funding situation in order to build an open source ProgPoW miner.

We have 2 options:

1. Delay ProgPoW until the hardfork after Istanbul.
2. Have ProgPoW as it's own hardfork to be implemented once the audit is done.

This is not an ideal situation at all, but despite our best efforts it is what we have before us.
This post was also posted in the AllCoreDevs Gitter chat (**https://gitter.im/ethereum/AllCoreDevs**) for further feedback.

2 Likes

---

timolson #35 May 30, 2019, 9:40pm

Hi, I've engineered both GPU and ASIC miners, and I've also operated large-scale CPU and medium-sized GPU farms. Together with 7400 and Salt, we released an open-source ASIC miner for **Cryptonight Classic** that was 5x better H/J than Bitmain's X1, while using only 28nm. Recently, the Monero PoW team invited me to review RandomX, and I'm also releasing new technical work on Cuckoo Cycle.

Our hardware team at altASIC has done an initial review of ProgPoW and posted our comments to their **GitHub issue**. We're unwilling to go on record as to whether ProgPoW will meet its objectives of keeping ASIC's to within 2x and thereby being considered more ASIC-resistant than Ethash. Such determination would require more implementation work than we are willing to commit, but we call attention to the published design by Sonia Chen at Linzhi, also referenced in the ProgPoW issue.

I've cross-posted our comments here from the ProgPoW issue, and hope they're helpful to the Ethereum community:

> Overall, ProgPoW looks to be a genuine, professional attempt by GPU-interested parties. That is to say, we found no obvious backdoors or any suggestion that ProgPoW is anything but an honest attempt at ASIC resistance.
>
> The inner loop does try to cover the shader datapaths pretty well, but obviously GPU's without a unified texture/L1 architecture will waste some texture area, and all geometry pipelines go unused. Also, ProgPoW is strictly integer math, while GPU's predominantly focus on float performance, so that overlap is also less than 100%. However, we are not GPU insiders and cannot quantify the GPU die area that would go unused in ProgPoW.

> We do point out that while GPU's are not especially good at integer multiplication and are outright bad at bit operations, five of eleven random math operations in ProgPoW are bitops and two are multiplies. For Nvidia, bitops take 2 cycles each, the same as addition, and multiplies are so slow the official docs say only "multiple cycles." In ASIC's, bit operations especially can run considerably faster.
>
> We suspect a VLIW architecture may help exploit this, by combining multiple instructions into a bundle that can be computed in fewer clock cycles than each instruction individually. If we group the 11 operations into three categories: bitops, adds, and muls (also rot), then our slow-seed compiler can generate instructions like bitop-muladd-bitop that frequently match branches of the abstract syntax tree and run in far less than the 8+ cycles this would take on a GPU. The timings and dependencies of instructions may be precalculated by the compiler, such that no on-chip sequencing logic is necessary. Also, the set of VLIW instructions may be generated from the distribution of the program space, and this distribution may also inform the number of compute instances for each instruction. There would be many bitop-bitop units for example, and fewer bitop-add-mul-add-bitop units, efficiently matching transistor count to the frequency of each op sequence.
>
> These gains all together may or may not give a 2x speedup, and we can't say without deeper analysis.
>
> Overall we think ProgPoW is a good try, probably the best anti-ASIC attempt so far. It is relatively simple and straightforward, and professionally designed and documented, yet we remain uncertain of its chances for keeping the ASIC gap to 2x.

2 Likes

---

timolson #37 June 1, 2019, 5:49pm

I'm not suggesting that the PoW use floats, and of course I'm well aware of the issues. Actually RandomX does use floats in a CPU-oriented PoW, but they take care to avoid non-normal conditions like underflow and NaN, and they've verified implementation consistency with the IEEE standard across Intel, AMD, and ARM, exhaustively validating all possible outputs of their float operators.

My point is that GPU's are primarily designed for floating point performance, not integers or bitops or flow control. In fact, the only operation that runs in a single cycle on an Nvidia card is a *half-precision* float muladd. Full precision float multiplies run in just 2 cycles even though their integer multiply counterpart is much slower. GPU's can do this because you just don't need exact answers in graphics shaders, only something that's close enough to look good to a human eye. GPU's do the best they can in a short time and leave some small errors in the LSB's of the significand, which is obviously unsuitable for a PoW. PoW's require exactness and integer arithmetic, and using GPU's for PoW is like using a hammer to drive a screw. The main thing they do well, float muladds, goes unused.

That is changing recently with the greater emphasis on GPGPU computing, but the focus is really on scientific compute and deep learning, which are both primarily all float ops. There is not much incentive outside crypto for GPU manufacturers to improve integer performance.

Although I want to maintain a neutral stance on ProgPoW vs Ethash, in general I think ASIC resistance is a fool's errand, and GPU mining is doomed. The ProgPoW team did what they could within the constraints provided, but you can't turn a boat into a car. Not their fault if it doesn't work. GPU's are just suboptimal for PoW computations.

ProgPoW's hope is that is they do get "close enough" to ASIC performance that the economics of scale in the GPU industry make smaller ASIC manufacturers unable to compete, but this is an Economy of Scale effect, not a technical difference between ASIC's and GPU's. ASIC's by their very definition will always be faster than general compute units at the task for which the ASIC was designed. The question is whether a GPU's integer performance is good enough relative to ASIC's to allow the GPU industry's economy of scale to make up the difference.

If GPU integer performance sucks very badly then ProgPoW may be worse than Ethash. If GPU's perform pretty well at integers, then ProgPoW may be better. We're not willing to speculate without a lot more work.

My personal view on PoW is that there is no such thing as ASIC resistance. Furthermore, GPU's can jump coins and are easily rented and are therefore less secure than ASIC's even before you consider hashrates. A PoW needs to be simple to understand and implement, and it needs to be well reviewed by serious cryptographers. IMO Ethereum should dump both ProgPoW and Ethash and use Keccak. But there's too much GPU-interested politics in Ethereum for that…

---

timolson #40 June 3, 2019, 6:24pm

FFS I try to post a highly-educated technical review and first get insulted that I don't even know the *basics* of floats, and now you think I don't know who Kristy is or understand that ASIC resistance is a continuum?

We specifically call out the 2x threshold which seems to be a common number used for "resistance" and also say it's not clear that ProgPoW is an improvement over Ethash (but it's an honest try.) Really, it could go either way. If you just care about delaying ASIC's with forks then the PoW doesn't matter much. Just keep forking to something new every 6 months. If you think ProgPoW will last 12 months then that is purely speculation.

I thought the community would want an expert opinion that didn't come from the authors. If you'd like to ask for more detail on our assessment I'm happy to oblige, but I have no interest in devolving into a philosophical PoW conversation. I shouldn't have said anything about my personal view on PoW.

To my knowledge, no one has mentioned or considered a VLIW architecture for ProgPoW before, and it's a clever approach that will give a nontrivial performance increase, so *you're welcome*. I could have sat on this design and made a lot of money selling a ProgPoW ASIC.

I find it strange that no one has yet commented on this VLIW proposal or its implications for ASIC resistance. Instead, you seem most interested in just quoting KLM to me and defending a philosophical position you were already entrenched in… Have you even bothered to add up the gate counts in Linzhi's design? Hmm? What do you get for your die area calculations?

3 Likes

timolson #42 June 2, 2019, 11:17pm

Sorry, it was my fault to say anything beyond the ProgPoW facts. I shouldn't be snippy.

When I say ASIC resistance is not possible, it is an *opinion* that "even economies of scale in GPU's or CPU's are not enough to prevent a 2x improvement by ASIC's in terms of total-cost-per-hash for any given PoW." I don't mean ASIC-proof; even a loose "economic resistance" seems too much. And even if 2x is achieved, I do not think that is enough to save GPU's. But these are personal opinions not ProgPoW facts.

Maybe ProgPoW proves me wrong. I'm open to that. Like I said, I think it's the best try so far, but I'm not sure if it's better than Ethash. It's a good try for sure.

Certainly ProgPoW is much more than an ECO on Ethash. It's an all-new chip for sure. But the spec has been around long enough that you should expect a great deal of ASIC design work to already be completed. You could see ProgPoW ASIC miners on the network within 4-6 months of a switch to ProgPoW being finalized. I would expect manufacturers to wait for certainty on ProgPoW before taping out, so it's actually to your benefit to keep alive the possibility of not switching. That's 4 months from *decision time*, not from launch time…

For a case study in forking to fight ASIC's, look at Monero. Their first attempt was useless (quickly ECO'd) but even big changes were overcome by ASIC's within 6 months or so. The thing currently keeping ASIC's at bay in Monero is the *threat* of further imminent forks, not anything to do with the PoW.

3 Likes

timolson #43 June 2, 2019, 11:33pm

A separate point about mining economics:

Many people assume hash-per-joule is the ultimate mining metric, but anyone who has run a mine knows that capital expense is actually a HUGE factor, because the lifetime of mining hardware is so short. Of course the total lifetime cost for a miner is capex + time*opex, so if time is short, capex dominates. It's a line with capex at time 0, going up with slope opex.

< *deleted some wrong speculation about ethash vs progpow in capex vs opex* >

ProgPoW will have both a bigger capex and opex cost compared to Ethash, so both the offset and slope of the total cost line will go up. That may seem like ProgPoW is an instant win vs Ethash, but it's not clear, because maybe ProgPoW ASIC's improve the slope of the cost line vs GPU's more than Ethash ASIC's. Then things depend on the lifetime you choose for the equipment, and the economic-ASIC-resistance lines of the two PoW's will cross at some point…

You need to basically *make* an ASIC in order to know its power and area well enough to compute the cost lines that would inform any economic-ASIC-resistance determination.

timolson #44 June 2, 2019, 9:13pm

Also, no one should worry about the audit firm dropping the job. It's a thankless task and honestly very little money. Generally you'd need something like $500k to $1m to do enough work to make specific power and area claims. With the amount you have in the fund, under $20k I believe, you shouldn't expect any real conclusion on ProgPoW to come out of the audit. Not sure what your specific goals are for that review.

timolson #47 June 2, 2019, 10:43pm

Let me emphasize the word "might" in all those capex/opex statements. It's probably not fair for me to conjecture. To explain:

Ethash primarily relies on bandwidth to memory with only very light computation, but ProgPoW adds a lot of computation, which means both extra silicon (capex) and extra power (opex). Actually it probably adds more to the opex side than the capex side, but I don't know, so I shouldn't have said anything. But yes they are using more chip, which means more up-front cost (capex), but there will be a lot more power too (opex). I don't want to speculate whether one or the other will be better for typical miner lifetimes, only to point out the complexity of calculating economic ASIC-resistance.

timolson #48 June 2, 2019, 11:02pm

> timolson:
>
> Ethash is designed to minimize opex and decrease the difference in H/J vs ASIC's, whereas ProgPoW has a significant capex component because of its large silicon requirement. However, ProgPoW might be sacrificing ASIC-resistance in opex to achieve its ASIC-resistance in capex

This is wrong BS by me don't believe it. In fact it's probably the opposite way around. I was thinking only about the silicon not the power… We won't know the power requirements of a ProgPoW ASIC without basically prototyping one, like I said above about the audit cost.

Sonia-Chen #50 June 3, 2019, 10:12am

[Disclaimer/Background: I work for Linzhi Shenzhen, a small independent privately funded ASIC startup in Shenzhen. We are working on an upcoming crypto chip whose first application will be Ethash, as announced at ETC Summit 2018 in Seoul. We are facing some delays, but all is fine. All things worth doing take longer than expected.]

In my view, **@timolson** did the Ethereum community a great - free - service with his series of posts and replies in this thread. Thank you Tim!

We at Linzhi are a little more open to speculating about the intentions or business deals that may have led to ProgPoW, which look very different from those behind RandomX. The anonymous nature of Mr. Else and Mr. Def as well as a number of surprisingly uniform accounts and articles/presentations are quite intriguing.
We don't know the deals between Core Scientific (where Kristy-Leigh Minehan the main ProgPoW proponent is CTO) and Nvidia. We believe cost advantage leads to centralization

> **ASICs and 51%—Achieving Mining Dominance How cost advantage drives...**
>
> We want to take time to explain why we think a change in PoW is risky for Ethereum at this point.
>
> Reading time: 5 min read

ProgPoW risks turning Ethereum into an Nvidia-managed game, with ETH devs becoming unpaid support staff to keep the game going.

I'm relaying the following quote from people with more GPU expertise than we have or are willing to acquire (not from Linzhi, take it fwiw):

"On AMD V_MUL_LO_U32 uses 16 cycles, on Nvidia starting from Volta IMAD uses 5 cycles.

32-bit multiplication in ProgPoW was pushed under the pretense of it being inefficient on both manufacturers but that turns out to be a lie as on Nvidia it was only inefficient on Pascal. The algorithm is tuned to still let Pascal utilize full memory bandwidth due to simply sheer compute capacity difference coming partially from higher die size which is why comparing GPUs based on price is being pushed as of late. It's not a secret that 4xx & 5xx series AMD GPUs are not high-end but because ProgPoW's compute to memory bandwidth ratio is tuned to match Nvidia GPUs, AMD GPUs are not utilized to their fullest, most importantly losing the full memory bandwidth utilization which is the very basic foundation of the Ethash algorithm."

Is this true? If so would it leave much of the "honesty of the attempt" that **@timolson** sees?

Phil Daian wrote a great paper over a year ago
https://pdaian.com/blog/anti-asic-forks-considered-harmful/

There is another anonymous guy out there writing about ProgPoW, ether4life (no, it's not us).

> 
>
>
> **#ProgPoW Follow-Up: The Cost of ASIC Design**
>
> I was glad to see that IfDefElse published an interesting article "The Cost of ASIC Design" as a response to my previous article. However, I think IfDefElse are not very familiar with ASIC design and...

ASICs are designed and manufactured when there are buyers.
Currently there is sufficient demand if a machine can offer 150 days ROI (with flat/flat assumption, that is coin price flat, difficulty flat).
ETH currently pays out 3.6 mio USD / day or about 100 mio USD / month.

Without doing much math, it's not hard to see how a system that pays out 100 mio USD / month can incentivize the design and development of chips. A lot can be done for a few million USD and it's only natural that different businesses are competing for that money.

@fubuloubu - prepared or irregular PoW changes are a big incentive for secret mining. The alternative would be to pre-announce a PoW change one or two years in advance.

Quoting **@timolson**
"If GPU integer performance sucks very badly then ProgPoW may be worse than Ethash. If GPU's perform pretty well at integers, then ProgPoW may be better. We're not willing to speculate without a lot more work."

+1 from Linzhi.

Tim made many other good points, I can tell you what I am doing: re-read his points, think. There are always new realizations to be had. What about the VLIW design? 🙂
We are happy to have more discussions also in our Telegram group LinzhiCorp.

---

timolson #51 June 3, 2019, 4:28pm

> Sonia-Chen:
>
> > ProgPoW's compute to memory bandwidth ratio is tuned to match Nvidia GPUs, AMD GPUs are not utilized to their fullest, most importantly losing the full memory bandwidth utilization which is the very basic foundation of the Ethash algorithm."
>
> Is this true? If so would it leave much of the "honesty of the attempt" that **@timolson** sees?

We did *not* look at the AMD vs Nvidia issue. When we say "honest attempt" we mean that ProgPoW doesn't have some secret way to make ASIC's easy, or any backdoor, or anything like that. It is definitely pro-GPU.

It may be true—almost inevitable—that one manufacturer or card series outperforms the other. It may be true that the authors have specifically tuned the PoW to favor Nvidia over AMD.

AMD vs. Nvidia may be tuned using ProgPoW's loop constants for compute and memory, and IMO it's up to the Ethereum community to test different values on different cards and decide what's fair. The structure and design of ProgPoW does not fundamentally favor either vendor in my view, and the tunings my be adjusted and tested by any GPU enthusiast who can change one number and compile code. If the Eth community doesn't want to do the simple work of trying different loop constants on different cards, then the hard work of fighting over what values are fair, then they can just accept the authors' suggested tunings. But don't be afraid to adjust the loop constants if you are concerned about GPU vendor bias.

3 Likes

timolson #52 June 3, 2019, 4:37pm

> Sonia-Chen:
>
> In my view, **@timolson** did the Ethereum community a great - free - service with his series of posts and replies in this thread. Thank you Tim!

Thanks Sonia, you too! Linzhi has also offered valuable free insight into ProgPoW including a basic ASIC design with gate counts, and they've been generous in also helping RandomX improve their effort. Sonia knows what she's talking about, and free advice in hardware is really rare. It's wonderful to see such entrepreneurial spirit and transparency!

Sonia-Chen #54 June 4, 2019, 8:19am

Linzhi's four core principles are: truth, learn from customer, innovation, customer trust.

@epic.henry

> Why can't we all be friends and have FUN 1 like SpongeBOB instead of spreading FUD like Plankton?

No. Don't try that. Don't like you.

EIP 1057 author bitcointalk trust page (need to login)
https://bitcointalk.org/index.php?action=trust;u=838402

EIP 1057 author employee review
https://www.glassdoor.de/Überblick/Arbeit-bei-The-Mineority-EI_IE2404190.11,24.htm

EIP 1057 author speaking at coingeek event

https://coingeek.com/kristy-leigh-minehan-bitcoin-should-work-but-not-be-seen-video/

DYOR

The best crypto ASIC related work lately in my opinion is happening in Monero, look for tevador, hyc, solardiz, Tim Olson and others.
They have secured funding and tasked 4 auditors with a review within days: Kudelski, QuarksLab, X41, TrailOfBits

r/Monero - RandomX Auditor Selection

87 votes and 47 comments so far on Reddit

One thought that is still rarely brought up is that “ASIC friendliness” just means repeating the “ASIC Resistance” pseudo-science one more time (third level maybe ASIC Assistance? 🙂).
The cost of making a Bitcoin miner is far higher than people think. Maybe we find time for a substantial article on this subject one day. We drove sha-256 from 8000 W/T to 100 W/T, we learned a lot.

@shemnon

> The main question are can we delay the entry of ASICs into a ProgPow POW ecosystem, but does the mechanism proposed to delay it in a fashion that makes economic sense. A two week delay fixed by a change order is a delay, but a pointless one. Is ProgPow a similarly pointless delay?

It’s impossible to find a satisfactory answer.

ETH mining is a multi-billion USD industry. At a high-level, if we assume a network capacity of 800 MW and 4 cents/kWh, that’s ca 23 mio USD monthly electricity cost. ETH payouts right now are 103 mio USD / month.
That means 80 mio USD/month gross margin. The small guys may be hurting and fighting, but the big guys are making good money.

Remember I said a machine sells (there is a buyer) when it’s priced at 150 days ROI flat/flat?
That answers the capex question that was brought up earlier.

We are happy to answer questions about ASICs and costs and mining economics, all publicly.
Hardware manufacturers optimize along 5 dimensions that are often mutually exclusive: cost, performance, efficiency, time to market, reliability.
They shouldn’t forget about complexity either, something we are learning right now 🙂
Cheers.

Sonia-Chen #55 June 5, 2019, 4:34am

@timolson

> It’s wonderful to see such entrepreneurial spirit and transparency!

Thanks. That means the mistakes are also transparent though.

In 09/18 we announced our Ethash chip schedule to be 12/18 tapeout, 04/19 samples, 06/19 mass production. Today we are in 06/19 and haven't taped out yet. That means we are 3+6=9 - 2x off in our tapeout schedule. If we are also 2x off for the rest of the schedule the machine won't sell for another year or more. If we are off by 2x on time-to-market, we can arguably be off by 2x on cost or efficiency or performance or reliability as well. We are just WRONG, and not happy about it. We haven't taken a single prepay order or dollar.
We will continue with the open process.

I wrote this elsewhere, the division of labor in ASIC resistance is best seen as someone claiming "X cannot be done", and someone else just doing it. Otherwise you are in an infinite circle of that other person saying "X can be done", and the original claimant repeating "X cannot be done".

We have always worked on the "just do it" side.

@epic.henry

> I would also chastise Linzhi to do their homework and check the facts before posting incorrect information.

Knowledge is power. Kristy/Core/Nvidia/nchain/epic is chastising for homework!
chastise = "rebuke or reprimand severely", "infliction of corporal punishment".
There is indeed punishment for people not doing their homework.
If "epic blockchain" is even remotely involved in the audit, we already know the result.

Some homework:

> **Least%20Authority%20-%20ProgPow%20Algorithm%20Audit%20Proposal%20(v2).pdf**

The areas of concern were listed as
(11) Other effects impacting the ecosystem at large (distribution, economies of scale, cost, etc) and other externalities of such a change.
(13) ProgPoW's ability to provide better decentralization

This just came in:
https://www.nasdaq.com/press-release/squire-enters-into-a-binding-letter-of-intent-with-core-scientific-for-hosting-of-blockchain-cloud-20190604-00893
https://www.bloomberg.com/press-releases/2019-05-30/squire-agrees-to-purchase-companies-with-cloud-computing-assets-totaling-2-985-petahash-to-become-one-of-the-world-s-largest

The EIP 1057 author stated this morning, linking to those news: "Core Scientific is killing it! Stay tuned for more massive announcements. This isn't the only one." (in Telegram, just believe me, or believe Nasdaq/Bloomberg).

Should we ask the EIP 1057 author whether some of those future announcements relate to Ethereum? What are the deals between Core Scientific and Nvidia? Core Scientific and Squire/Calvin Ayre/nChain?

The auditor better look into that (areas of concern 11 and 13), if you don't want to be surprised by news from Bloomberg one day.

We think the current ETH mining is quite stable and decentralized, with at least 4 vendors having competitive chips (AMD, NV, BM, Inno), and at least 5 others working on chips. That's exactly why some parties who don't like fair and decentralized mining are working towards centralization. ProgPoW is their tool. It's an interesting process to see this battle between centralization and decentralization unfold.

---

fubuloubu #58 June 5, 2019, 1:38pm

> Sonia-Chen:
>
> 4 vendors having competitive chips (AMD, NV, BM, Inno), and at least 5 others working on chips.

Questions (if you are still being transparent):

1. Are AMD and Nvidia working on future mining-only chip designs? If so, do you have link to public release documents.
2. Are these the latest **BM**/**Inno** miners? Are there more available privately? Are they doing any private mining with more efficient hardware that is to be released?
3. If there are 5 others working on chips (I assume you are one of them), how close are they to be production? How much more efficient will they be? Will they self-mine before release for "quality assurance purposes"?

Interesting questions I'd like to know, if you are being so transparent so as to help us along.

1 Like

---

timolson #59 June 5, 2019, 9:38pm

Proposal to Alleviate Any Conflict-of-Interest by the ProgPoW Authors

If the community's problem centers around the authors' alleged business interests, then **change the loop constants**. I can't emphasize this enough. There could be a straightforward community effort to collect the best ProgPoW tunings for a variety of popular GPUs, then decide on something that's "market fair."

I've seen charts that quantify the power-per-hash using the *current constants*, but that metric doesn't consider % of resource usage for each card. Yes H/W might be the same across cards, but the overall hashrate on some cards will be artificially low (and still proportional by power).

If such information is not already available, we **need** a chart of the optimal values for `PROGPOW_CNT_CACHE` and `PROGPOW_CNT_MATH` for a variety of popular GPU's. The optimal loop constant values are the smallest numbers which give a "saturated" maximum hashrate on the card.

This requires use of the vendor's devkit telemetry tools, but a simple recipe and test harness could be made to allow home GPU enthusiasts to try all combinations. With a spreadsheet of GPU cost, power, hashrate, and optimal loop constants, the community can make an informed, transparent decision on the values for the two loop constants, and thereby openly divide the market based on different GPU vendors' capabilities.

2 Likes

Sonia-Chen #60 June 6, 2019, 1:04pm

@fubuloubu

Thanks for asking.
I work for a small self-funded chip startup, we are a bunch of folks in a small office in Shenzhen basically. My answers to your questions are "market chat", things we hear, think, guess, calculate.

> Are AMD and Nvidia working on future mining-only chip designs?

I doubt it. Agree with **@timolson** "using GPU's for PoW is like using a hammer to drive a screw". GPUs are good to secure small networks or new coins, and for development.
For now PoW chips are fixed-function, they tend to have much lower margins (utility chips) and are thus not interesting for Nvidia. Therefore, Nvidia will focus efforts on marketing to create enough instability to deter ASICs and to keep the mining revenues on GPUs through forks (btw, in our view the competition between Nvidia and AMD is largely for show, to keep antitrust regulators happy, but that gets us into politics and totally away from technology).

> If so, do you have link to public release documents.

No.

> Are these the latest BM 1/Inno 1 miners?
> Are there more available privately?

I'm combining these two questions.

Let's assume a vendor will always try to sell their most advanced product. I think neither Bitmain nor Innosilicon are currently offering Ethash machines. I contacted them through a friend this morning, just asking for a quote - anyone can do this. We do know both Bitmain and Innosilicon are "close" to a competitive offering, technically. Bitmain has sold 20k E3 (our latest estimate), Innosilicon decided not to sell/offer for sale.

I want to take the time to walk through the economics, using Bitmain E3 as an example:

Why is the E3 not being offered anymore? When will it be offered again? At which pricepoint?
Those questions can be answered rationally, excluding a few exceptional things like insolvency, unsold inventory blocking the market, willingness to loose a lot of money to bankrupt a competitor, trade wars, politics, etc.

We need to know three things: cost, margin, ROI.

1. Cost
   Since the E3 is a close competitor to us, we spend some time to analyze its cost. We get a machine, take it apart, think about it, and put some numbers into a simple spreadsheet. The key cost component of an E3 are the 576 memory dies. At the very lowest, we can imagine cost of 40 US cents / memory die (most likely it's higher).
   We calculate a lowest-possible E3 machine cost of 840 USD.

2. Margin
   Nvidia needs a gross margin of 60% to be happy (you can take this number from published financial reports). Any new business (sales) with a lower margin is bad for Nvidia, any new business with a higher margin is good for Nvidia.
   We don't know the margin Bitmain is targeting, but let's just put it at 30% for now.

3. ROI
   The current ETH networks pays 2.15 cents/MH/day (**bitinfocharts.com**)
   We assume an all-in power price of 4 US cents (that's a realistic number for the purpose of this calculation, just believe me)
   An E3 that hashes 190MH at 800W thus generates 2.15 * 190=4.08 USD at a cost of 24 * 0.8 * 0.04=0.77 USD for gross revenue of 3.31 USD / day
   The machine sells, in the current market, at 150 days ROI flat/flat (again just believe me), that means 150 * 3.31 = 496.5 USD

Now we can put it all together:

At the current Ethash profitability, Bitmain would need to offer the E3 at 500 USD to find a buyer, but it wants 840 * 1.3=1,100 USD. Noone will order, Bitmain won't even offer, nothing happens.
How high does the Ethash profitability have to go for E3 sales to restart: 1100/150=7.33 USD/day + power .77=8.1 USD/190=0.0426 cents/MH/day.
At the current difficulty, that would mean an ETH coin price of 246*(0.0426/0.0215) = 488 USD.

We got it! **E3 sales will restart if ETH goes back to 488 USD** 🙂
This may be impacted by irrational assumptions aka "risk taking" by certain market participants, but by and large this gives you a good mental model to relax and watch what's happening.

> Are they doing any private mining with more efficient hardware that is to be released?

Who can rule this out after all that happened in recent years.

Who is to say that "they" must be the ASIC designers or manufacturers. It could also be the ASIC (or GPU) buyers that want to do private mining with more efficient hardware that they have secretly acquired. You may remember tweets of the EIP 1057 author directed at you (since deleted)

- *"Genesis Mining and others also benefitted heavily from private optimisations for 2+ years"*
- *"I even traded VBIOS' for hardware discounts"*

Yes this is mudslinging, but since an unfair story is repeated forever ("greedy chinese asics"), you might as well hear the other side once in a while.
We know who comes to us and tries to meet and tries to buy, and what they want. Some ETH community members should be flies on the wall, that'd be fun…

I know this is annoying, but it's a fact that the EIP 1057 author is doing big business deals with Calvin Ayre's and Craig Wright's companies (just read the news, linked in the last post).
Whether mining becomes more transparent or more private is a consequence of the aggregate decisions of the community.
In a community that prefers theories over business scrutiny, business people will continue without oversight.

> If there are 5 others working on chips (I assume you are one of them),
> how close are they to be production?

We are transparent, we are trying this. We are very far from production 🙂
I want to reiterate a general invitation to our office and factory in Shenzhen. ASICs are fun, a lot to learn. Let's go through the others - market chat…

1. vidtoo in Hangzhou: even further from production than us
2. Ingenic in Beijing: just starting with crypto, confused about Ethash vs ProgPoW, even further from production than us, but don't want to underestimate them
3. Samsung: May be the real reason of Nvidia's ProgPoW effort (in addition to excluding Bitmain). Instability will keep them away.
4. unknown (to us) team working with Xilinx ZU6EG/9EG: Since ProgPoW has a lot more logic than Ethash, it has brought some FPGAs back in play. We don't know many details about this effort or how it would work for Ethash, but the team is real afaik. If ProgPoW progresses, I would love to hear from people who take a serious look at the ZU6EG/9EG and are willing to share their findings openly.

I admit that I don't have a specific fifth one for you. The entire sentence reads "We think the current ETH mining is quite stable and decentralized, … with at least 5 others working on chips." You bet there are at least 10, 20 or more "others".
In Shenzhen alone we have about 1000 semiconductor startups. Maybe people forgot the garages. The beauty of PoW chips is that you immediately have great constraints to focus your design skills on. Professors all over semiconductor classes are saying "This semester we are going to design an Ethash ASIC", and the students say "yeahh… coool…" 🙂 Then you have existing chip businesses with under-utilized design teams who need to be kept busy, so why not try a PoW asic?

Bottom line: Noone is close to production.

> How much more efficient will they be?

OK the crazy fun answer first: ETH DAG size increases linear, but semiconductor density increases more than linear. How about a single-die 5nm chip generating 20 GH hashrate? How about 3D chips, high-density wiring between dies, silicon photonics?

More seriously, your question asks for an economic answer: As much as the monthly payouts for Ethash (or ProgPoW) increase, efficiency gains will be made. However GPUs are holding up well against E3 and A10.

How easy or hard is it for higher-efficiency machines to push out lower-efficiency machines?
Before we calculated that E3 sales could restart if ETH coin price reaches 488 USD.

Let’s calculate how low coin price can go before the big GPU operators would be pushed out:
Let’s take a GPU average of 30 MH at 150 W (there is quite some variance in this).
Daily power cost: 0.15 * 24 * 0.04=14.4 cents
Daily revenues: 30 * 0.0215=64.5 cents
246/(64.5/14.4)=54.92 USD

So in this way of calculating, ETH price could go as low as 55 USD! That shows how strong the position of existing machines is, once they are paid for and installed.
Let’s try another way of calculating recycling resistance, from SHA-256 machines: We know the Avalon machines best because we designed and manufactured them. Here in Shenzhen nothing gets wasted, we see the parts of our old machines in the parts market, then we know the recycling situation. We are certain that all A6 have been recycled, we are guessing about 50% of A7 have been recycled, and we think no A8 has been recycled yet (we haven’t seen A8 parts in the used parts market).

I’m using averages: A6 = 3.5T@1100W. A7 = 6.5T@1000W, A8 = 11T@1200W.
At power cost of 0.04 cents/kWh, and current SHA-256 rewards of 27 cents/TH/day, it looks like this:

A6 (100% recycled): 3.5 * 27=94.5 cents revenues, 24 * 1.1 * 0.04=1.06 USD cost.
94.5 < 106 : 100% recycled

A7 (50% recycled): 6.5 * 27=175 cents revenues, 24 * 1 * 0.04=0.96 cents cost.
175 > 96: 50% recycled

A8 (0% recycled): 11 * 27=297 cents revenues, 24 * 1.2 * 0.04=1.15 USD cost.
297 > 115: 0% recycled

This gives us a lot of confidence, it looks right! Some people have higher power costs, lower power costs. Higher or lower labor or capital costs. But in the end it all has to come down back to earth.
For ETH, there is a lot of variance in GPU performance, and GPUs will continue to improve. If an E3 needs 488 USD/ETH to sell, but (some) GPUs by (some) operators can still be profitably run at 80 USD/ETH, that means the E3 will not push out GPUs anytime soon.
The pain you are hearing from GPU operators at 150 USD/ETH, 120 USD/ETH, 100 USD/ETH and lower is the small GPU guys hurting from competition with the large GPU guys. It has nothing to do with ASICs.

Bottom line: expect incremental efficiency gains, because theoretical efficiency gains are held back economically.

Thinking about these numbers may be a bit depressing. The ETH community shuffles hundreds of millions of USD to some very weird business people and megafarms. If the community cannot or doesn’t want to stay in control of this, or thinks it can do better with less waste, then switch to PoS faster.

> Will they self-mine before release for “quality assurance purposes”?

Depends on what the community or the customer of the manufacturer wants. We are open to community oversight, just board a plane to Shenzhen.
Why do we try an open process? Because we don’t believe in fixed-function chips and are targeting programmable chips for which we need to cowork with developers.

Hope this makes sense, thanks again for asking.

Final Thoughts:
I'm sure I made mistakes in this post, some numbers wrong, some thought paths wrong. So what, we are learning. At least I'm sharing something. Maybe it's helpful to an auditor.
The ProgPoW team is also fun, once you can decode their language. Kristy, Henry, Jon Stevens, Jean Cyr, Teddy, Amel, Sarah, Heisenbug, Greerso, etc. - ha ha.
The details of their corporate scheming don't matter because we will most likely never see leaked contracts anyway. What's happening is obvious though, just do research, read news, connect the dots.
Yes the community should turn those knobs and make sure mining is fair, but it won't be enough to address the deeper problems of GPU mining in that large companies such as the one where the EIP 1057 author is CTO can gain an unfair advantage because they have co-opted the community to monopolize the supply chain for them down to the one chip vendor they have hooked up with. The solution to that is to bring Samsung, Bitmain, Inno and small guys like Linzhi in to decentralize. A self-serving argument 🙂

For reference here is a collection of writings of team ProgPoW, maybe someone can run some stylometry over this.
Dust off your bitcointalk password, login and check out the trust page of the EIP 1057 author. Follow other links. Do your homework.

20180518 **https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1057.md**
20180530 **https://medium.com/@OhGodAGirl/the-problem-with-proof-of-work-da9f0512dad9**
20180602 **https://medium.com/@OhGodAGirl/thank-you-alexander-for-your-constructive-feedback-d39078079186**
20181025 **https://medium.com/@ifdefelse/understanding-progpow-performance-and-tuning-d72713898db3**
20190111 **https://medium.com/@ifdefelse/progpow-faq-6d2dce8b5c8b**
20190207 **https://medium.com/@ifdefelse/re-my-take-on-progpow-d8a30a68f6da**
20190330 **https://medium.com/@ifdefelse/the-cost-of-asic-design-a44f9a065b72**
20190330 **https://medium.com/@profheisenberg/everybody-knows-alus-are-relatively-tiny-circuits-a589d2de4cce**
20190318 **https://medium.com/altcoin-magazine/13-questions-about-ethereums-movement-to-progpow-e17e0a6d88b8**
20190327 **https://medium.com/altcoin-magazine/comprehensive-progpow-benchmark-715126798476**

---

timolson #64 June 12, 2019, 9:24pm

> epic.henry:
>
> Thanks for all your hard work pulling the analysis together. It must have taken days of benchmarking, reconfiguring systems and tuning memory clocks. I thought your article would have put an end to the AMD vs Nvidia argument but the FUD and mudslinging continues.

Sorry, but unfortunately I think **@xazax310** 's benchmark is not what is needed, and it's probably misleading.

First off, it looks like he only tested one program (a single block height.) Any single program may have a non-representative distribution of math operations, so *many* possible block heights / programs must be tested and an average taken.

Secondly, as I mentioned above, merely optimizing the hashrate & power per card does nothing to show whether the card is near 100% utilization on all resources. The ProgPoW authors could have tuned the loop constants for Nvidia cards, and xazax310's benchmark would not show the bias.

This is not FUD. I have zero interest in Ethereum politics. I own zero ETH and do not mine it. If you want to claim that the ProgPoW authors have no Nvidia bias, follow the proposal I wrote above, which requires modifying the loop constants and testing GPU *resource utilization* NOT total hashrate or hash-per-watt. Do the ProgPoW authors' proposed constants cause higher utilization on Nvidia cards vs AMD's? xazax's benchmark does not answer this question.

Sonia-Chen #79 July 14, 2019, 5:04pm

I may dissent, and a few more links for the studious among us:

- **Voting and Miners**

It's unfair to equate the ProgPoW team with miners. The ProgPoW team doesn't represent the interests of honest miners at all, and voting was heavily rigged and manipulated in favor of ProgPoW.

One random example, a voice of the suppressed:

> **All these "votings" are not representative at all. - Кирилл Вакулин - Medium**
>
> Let's take Ethermine for e.g. What's they did? They just took all availabale hashrate, without any notifications for miners, and started…
>
> Reading time: 1 min read

> "Let's take Ethermine for e.g. What's they did?
> They just took all availabale hashrate, without any notifications
> for miners, and started voting YES. They promised provide dedicated
> port for say NO, but didn't provide it.
> In this situation, miners were just hostages of pools.
>
> If you want fair voting — at first prepare two different
> dedicated ports for YES and NO, and then start voting.
> Using default pool config for "YES" — it's just fraud!"

James Prestwich got it

James Prestwich (_prestwich)

proof of work is intended to make honest actors profitable, and dishonest actors unprofitable

which is why Ethereum is switching to ProgPoW in order to punish honest miners

wait what?🤔

2:36 PM - 22 Mar 2019 ♥ 74 ↻ 14

In PoW, lowest cost wins.
“Permissionless” access to hardware doesn’t help if you can buy GPUs at retail price in a lot of shops around the world, for a guaranteed loss.
Or you can be the one special partner of the chipmaker who helped the chipmaker exclude other chipmakers, and get the same GPUs at half the price or less in return.

- **Audit**

The last audit proposal I’m aware of is still this one

Least%20Authority%20-%20ProgPow%20Algorithm%20Audit%20Proposal%20(v2).pdf

Curious if that has changed.
What we’ve learned from the RandomX audits so far is that the first thing you want to see from an auditor is a one-page or more explanation of the **difference between a PoW algorithm and a cryptographic hash algorithm**, as seen by the audit team.
If the audit team doesn’t see any difference, or is just guessing a bit and largely thinks they are reviewing a cryptographic hash algorithm, that will lead to a disappointing result.

Report-X41-20190705.pdf

381.40 KB

This is not enough.

EIP 1057 makes some key claims that are demonstrably false, and yet were used to rally support behind the EIP, for example

> “These would result in minimal, roughly 1.1-1.2x, efficiency gains.
> This is much less than the 2x for Ethash”

That’s only the tip of the iceberg of this fraudulent EIP, but one would hope that an audit can keep more damage away from Ethereum.

- **Reputation**

The fact that the EIP 1057 author is a close business associate of Calvin Ayre and the nChain camp is public knowledge today, and seems to be accepted for now.
How do these guys make money?
Step 1: Sell ETH short on bitmex and other exchanges
Step 2: Put out press release saying Craig Wright co-authored and patented ProgPoW
Step 3: profit

- **Hardware Accessibility**

I was seriously surprised (and learning!) that someone could turn around the positive idea of not wanting to sell PoW hardware to ponzi schemes, scammers or money launderers into a “blacklisting” argument, and use that to instill more ASIC fear! Amazing.

Here’s what happens if a PoW hardware maker acts irresponsibly:

A rogue megafarm is selling hashrate to unsuspecting retail customers at excessive setup and maintenance rates, and thus ‘inherits’ the capex for free after a few months when the difficulty goes up and the inability of their customers (victims) to calculate becomes apparent.
They then proceed to destroy or otherwise manipulate/dominate that coin since their focus is on short-term profits.
A hashrate owner that obtained hashrate for free, through whatever means, is a threat to the coin.

Responsible chipmakers don’t sell to these kinds of farms, because they act against the long-term interests of the coin that is being secured.
Nvidia focuses on the short-term, since everybody knows that GPUs stand no chance in a PoW algo in the long run.

Sonia-Chen #93 July 16, 2019, 4:49pm

> One just needs to look how hard they are fighting to blackball this proposal to get a sense of the tactics that will be used in the coming years to oppose the transition to PoS.

“They” is me? We are the smallest and most insignificant group of all in this game, that’s why we can speak freely.
We are 5 people in Shenzhen, feel free to visit us. The tactics of team ProgPoW are tough, I have sympathy for the significant amount of time you invest in this and that you believe them.
It’s a nice campaign and attack pulled off by ProgPoW, and for sure they will never stop. The moment you hand them a mic, the story is back on.

For the record here is what we wrote on January 12th

> **ASICs and 51%—Achieving Mining Dominance How cost advantage drives...**
>
> We want to take time to explain why we think a change in PoW is risky for Ethereum at this point.
>
> Reading time: 5 min read

We are happy with the aging.
After discussions and news in recent months, it's a given for us now that ProgPoW is a corporate money-making attempt, brought to you by one mega-miner with special deals with Nvidia on the chip side, and Calvin Ayre/nchain on the customer side. GPU miners not part of the collusion between Nvidia and Core Scientific will suffer.

We are not in 2015 when Ethash was designed and audited. Today Ethereum pays out 100 mio USD / month for decentralized PoW security.
The days of "low barrier of entry to mining" are over unless Ethereum dramatically changes the incentives and PoW algorithm (not to ProgPoW, to something that actually does what it says).
The minimum size to be viable is 10 MW today.

> Use the threat of an algorithm change as a deterrent to further ASIC development

Our Ethash ASIC development will continue.
We are a chipmaker. We don't design chips for or against Ethereum, or for or against Ethereum Classic, Zilliqa, Bitcoin Cash, etc. I will happily work on long-form answers to serious questions such as what drives our chip decisions, what is hard and easy in chip design, what is costly and what is cheap, what the customers want, what about prepay, what about risk wafers, etc.
We are also learning, it's painfully obvious that our time estimate back from the ETC Summit was wrong!

It would be far more interesting to discuss how an Ethash (or ProgPoW) asic could lead to chips that accelerate ETH2. The investment carries over, so even if there is zero market for Ethash or ProgPoW, then the technology will be used to accelerate ETH2.

Sonia-Chen #107 July 17, 2019, 2:51pm

@elliot_olds

> what are we more worried about, people from outside the ecosystem attacking Ethereum or mining companies attacking it?

Are Core Scientific and nChain inside or outside the ecosystem?

I think you want to decrease the chance of attack (increase the cost of attack) of any single entity, whether inside or outside the ecosystem.
The best way to get there is sustained competition between as many parties as possible aiming for both cryptographically and thermodynamically provable PoW. "Parties" means anyone from chipmakers to machine/system integrators to hosters/miners/mining companies to mining pools.

> Despite my disagreements, Kristy deserves props for engaging with the arguments of ProgPow opponents.

Kristy is your attack vector, from within.
They created the problem (threat) they are now pretending to fix. When someone comes and tries to solve a problem that doesn't exist, think harder. You may need to do more than just say "no thanks".

When the ASIC fear campaign started, global Ethash hashrate was 265.8 TH (May 30, date of the article), and today it's 177.9 TH. Why?

The #1 problem with PoW: It's open to the kind of social attack ProgPoW is pulling off. If you are loosing on the hashrate, who said you can't try something creative to fight back?

> [Linzhi seems to be] quite small and without much influence

True, and good. PoW is a service to the network.

> For instance miners coming onto the dev calls to lobby for this and being treated as just normal concerned community members.

Have you found out the identities of Mr. Def and Mr. Else?
Does the community agree with the verification slowdown due to ProgPoW and its impact on light clients?

ProgPoW was kicked off by Nvidia, initially staffed with about 15 people in total. It seems to be a rather standard attempt by Nvidia to control a market using proven marketing. Forget what they say about being volunteers and the fake disclaimers under their articles.

> attacks from ASIC miners rather than external actors.

You mean "ASIC miners" as in people already running Bitmain E3 today?
Hashrate is impartial, you always want the hashrate distributed between as many different parties as possible (logically and physically separated).

Maybe you are assuming that someone who is already mining on the network today is less likely to attack than a new/external miner?
In that case you are excluding the possibility that ProgPoW was brought forward by one large existing miner to become even larger, and be able to dominate the network and extract value at will.

The chance of an existing miner with known-good intentions today turning bad is equal to the chance of a new miner joining with either good or bad intentions from the beginning.

> doesn't really engage with the issue of how the cost for an external actor to attack the network is higher with ASICs

Buying hashrate is always the most expensive (and for new hardware also slowest) way to attack a network. From most to least expensive you have: **1. buy 2. rent 3. steal**
There are some smart (as in business-smart) ways that are close to #3 such as financing a purchase and then not paying.
ProgPoW is also close to #3 because it steals hashrate from the network by excluding ASICs and

thus increases the relative share of the hashrate of the ProgPoW proponents.
ProgPoW thus reduces the attack costs (which I believe is the intention).

I believe the best way to increase (internal or external) attack cost is competition between chipmakers, but I should think about a long-form article to make that point.
If all parties (from chipmaker to pool) are under competitive pressure, noone will be able to accumulate enough profit to dominate the entire system.
There will be no centralization, and attack costs will be high.

> What we're really trying to do is lower the probability and severity of future attacks on Ethereum.

ProgPoW increases the probability and severity of attacks.

> This article is the kind of thing we should have been debating before ProgPow got the tentative go-ahead.

You didn't?
Some comments, quoting the article (KLM for Kristy):

> > KLM: The equation for [PoW's goal of preventing network centralization] was a combination of cryptographic math, philosophy, psychology and resource costs inherent with hardware

It is a combination of cryptographic math and thermodynamic competition.

> > KLM: [ProgPoW] is designed to target a critical part of the centralization problem: specialized hardware.

Red herring. The definition of specialized hardware doesn't hold under any kind of critical analysis. It's meant to distract from the fact that GPU mining machines are as specialized as ASIC mining machines.

The GPU chips that are used for Ethash mining today are built into highly specialized hardware, from special firmware to specially tuned memory to special cards to special machines. None of it is resellable or reusable outside of mining.

Rationally thinking about hardware means thinking about cost, hashrate and power consumption. Then there is also order lead time and reliability, but they seem to be of lesser importance in the Ethereum PoW context.

> > KLM: Specialization comes from removing unnecessary parts of hardware

Contradicts her own F1 racing car example later on. If you keep removing from a 4WD, will you eventually have an F1 car?
Specialization comes from designing a machine with only one goal in mind.

> KLM: When people talk about ASIC resistance, what they really mean is “centralization resistance”. That’s an important distinction to make, because the problem isn’t the hardware itself — it’s the companies and incentives behind it.

Yes. What are the incentives of Core Scientific?

> KLM: network security is relative to the amount of energy spent

Network security is relative to the amount of energy spent *efficiently*.

> KLM: Making specialized hardware means you’ve gamed the mining metric in a way that encourages everyone to buy more

Buy more until a maximum is reached. That is called competition, and why PoW is not only cryptographically, but also thermodynamically provable.

> KLM: [analogy of a car race between a 4WD and an F1 racing car]

The F1 analogy fails to think through the alternative: If everyone is forced to stay with the 4WD (GPU), the attack vector (the F1 car) is still possible technically. The security (inability to be outcompeted) was reduced.
PoW is thermodynamically provable, or it’s not PoW.

> KLM: The energy-to-work ratio is the same. The network isn’t anymore secure.

Who is the judge to check that none of the 4WD got any secret tuning?
The network is more secure if the competition is open between the 4WD and the F1, because an attack vector (the F1 car) was eliminated. And maybe the higher reliability of the 4WD means it’s more competitive to the F1 car than anyone would have thought.

> KLM: Bitmain is a corporation, and that means it has a duty: to maximize returns for investors. They’re chasing their incentives, and that incentive is to make money.

s/Bitmain/Core Scientific/

> KLM: Creating incentives for the security mechanism to dominate the network growth is just, well, letting the tail wag the dog.

Right, that's why ProgPoW should be rejected. PoW is a service to the network, not the other way round. ProgPoW is the tail wagging the Ethereum dog.

> KLM: This means the first manufacturer of custom hardware naturally has full control of the hashrate

This is already proven wrong by how long it took to bring the Bitmain E3 (and then Inno A10) to market and the lack of competitiveness with GPUs. I did a lot of math around this earlier in this thread.
Even if the ETH coin price would jump to 5,000 USD today, the network would still be secured by the same installed base of over 5 mio GPUs and it would take at least a year or more for ASICs to gain significant hashrate share. Before then even more GPUs would have rushed into the market bringing the difficulty up and slowing down the income of ASICs.
None of this touches any of the software devs' ability to change anything - protocol, PoW algo, mining rewards within a much shorter timeframe, if they want to.

> KLM: By impeding the network (see the empty-block example above), these miners and hardware manufacturers become the attackers by extracting value to the detriment of the network. Worse, their attack on the coin is constant and pervasive — a cancerous element that extends even to blogs and forums outside of the blockchain, where they spread misinformation and fearmonger to hide their motives and damage they do.

Freudian slip.
To be more blunt: That's the most vivid executive summary anyone could imagine about ProgPoW.

> KLM: Specialized ASIC makers and the miners who buy specialized hardware have guided the evolution of Bitcoin into a version of the traditional banking system, where they now hold all the keys.

Double false. First, the author is (today) CTO of a specialized machine mining company, and yet it's not enough to dominate and profit, so they are trying community infiltration and PoW change instead.

> KLM: As GPUs drop off due to loss of profitability, centralization will accrue around specialized hardware creators. Once this happens they can use attacks…

Circular reasoning at its best. How did the GPUs end up where they are today? Why is the "specialized hardware" somewhere else? Who are "they"?
This makes no sense at all. Specialized hardware is a misnomer, Kristy has expressed many times how fond she is of her drive towards specialization, how open minded about ASICs, etc.

> KLM: Specialized Defenses: Some would suggest algorithm stacking — found in coins such as RavenCoin, where the algorithms are repeatedly chained in randomized orders.

> However, Baikal has proven with their hardware (specifically the BK-X) that a bit of silicon area for each algorithm is all that is needed (and a sequencer, to distribute the order)

For RavenCoin, it's just "a bit of silicon for each algorithm and a sequencer to distribute the order". But for ProgPoW, it's guaranteed to be proof-of-GPU. Really?

> KLM: every algorithm that exists today has an optimal 'design' in hardware that can't effectively be surpassed

Obviously false. Is this worth discussing?
You are either designing an algorithm for a chip, or a chip for an algorithm. If you don't change the algorithm, the latter will always beat the prior thermodynamically.
We wrote a nice 5-step article how we would find a good (the best we can think of) design of a chip for a given algorithm.

Studying the Feasibility of an ASIC - Linzhi ASICs - Medium

Can you make an ASIC for algorithm X? How fast can it be? Can it be better than Y?

Reading time: 3 min read

> KLM: That's the key to decentralized mining — leverage existing markets which are bigger and already decentralized. When your hardware isn't specialized, the hardware starts, and stays, distributed.

Doesn't explain why Nvidia would leave money on the table. Throughout their 25yr history of gaining a 70% market share in GPUs they have demonstrated a ruthless attitude to making money.
Given its history we must assume, and ProgPoW proves, that Nvidia will try to keep mining centralized with them, gamify Ethereum and turn devs into unpaid support staff.

> KLM: to adapt the math in infinite and unpredictable patterns

It can't be that unpredictable, because it has to be verifiable.

> KLM: Once you understand how economic incentives help or harm cryptocurrency networks, it's easy to see how best to keep things truly decentralized

Right. Cost advantage leads to centralization.

Sonia-Chen #113 July 18, 2019, 7:58am

@elliot_olds

> They [Kristy] might know some factors that affect incentives that aren't obvious to people outside of the industry

You talked about governance. People always speak the truth? Lies don't exist?
Imagine a discussion between an engineer and a salesman, but the salesman pretends to be an engineer.

> The fact that you can rent GPUs from AWS and other generic cloud providers reduces the cost of an attack

Such non-mining GPUs are not built into specialized mining machines and stand no chance to compete with specialized GPU mining machines.

> I think what makes for piss-poor discussions is people acting defensively whenever a CoI is mentioned, and acting like it's some sort of assault on their character.

We live in the Trump era. If someone counter-attacks to a reasonable question, you have to draw your own conclusions from that.

> the interest of miners do conflict to a higher degree with the interests of the broader community, especially as it relates to ProgPow

ProgPoW is not in the interest of non-Core Scientific GPU miners.

@fubuloubu

> Kristy and a host of other supporters can't say a lick about ProgPoW without being painted with that scarlet letter.
> … it's much more productive to come up with logical reasoning why someone's facts or opinions are wrong
> … not a substitute for engaging in reasonable discussion.

Well we did a lot of work on that front, but I doubt many read it.
You cannot prove someone wrong who is intentionally lying from the beginning. Can you prove a politician wrong? They are structuring their entire sentences, from first to last word, to be un-disprovable.
You can logically reason about what you hear, and have a reasonable discussion, but eventually you will come to the conclusion that the other side is just lying. Not seeing this possibility is naive, not thinking it applies to Kristy-Leigh Minehan is fair. Everyone will eventually have a few people who believe them.

Let's do a little more homework, I love this. Yesterday I pointed out some things in the "Problem with PoW" article.

One key argument in the article are the many references to “specialized hardware”.

Here’s what Kristy said about specialized hardware a few weeks ago (June 24, 2019, quotes from the video):
https://coingeek.com/coingeek-toronto-conference-2019-kristy-leigh-minehan-on-bsv-mining-video/

> [7:33] Mining + Specialization = $$$
>
> KLM: This is something I uphold very dear to myself.
> KLM: Specialized infrastructure has been at war with the home miner.
> KLM: So one of the things we do at Core Scientific is we invest heavily in infrastructure, and specifically we invest heavily in specialization.
> KLM: The other piece is optimization. So one of the things we also specialize in at Core Scientific is specifically reverse engineering firmware, figuring out how can we get more optimization out of it.

She actually says that she is at war with the home miner! 🤣
If you ask her, maybe she will tell you it’s all different for GPUs (this talk is about BSV). Of course it’s the same for GPUs!
She will never stop, and it kind of makes sense. Why stop?
You want to avoid that Ethereum will be controlled by nChain and Calvin Ayre/Craig Wright.

OhGodAGirl #122 July 21, 2019, 10:27pm

Hi Sonia!

Your obsession with me is kind of creepy, still. Yes, I speak at conferences. Yes, my thoughts and opinions change based upon my experiences (good lord, what a shocking revelation!). Yes, for years, specialized infrastructure has been at war with the home miner. This is because specialized infrastructure generally has much larger economies of scale and pushes home miners out of the space. This is why infrastructure providers will slowly become service providers - the home miner will ‘join them’ and leverage their economies of scale and engineering effort, in the same way one leverages AWS or GCP.

It still disappoints me that after half a year, you're still acting like an emotional individual rather than as a company. Multiple people in this thread - including some that are highly respected in the fields of ASIC development - have gone out of their way to engage with you respectfully. You proceed to attack them, no rhyme or reason. You do nothing to cultivate trust in your company or product for foreign markets. Taking statements out of context or attacking an individual relentlessly doesn't do a single thing to assist you. In fact, all it does is reflect poorly on yourself and your company. Your continued behaviour echos true of the statement IfDefElse made two years ago - single-purpose hardware manufacturers will go out of their way to protect their investments, *whatever the cost.*

Everytime you attack myself, you strengthen ProgPoW and its merits - because if the best criticism that can come from it is my involvement, this will be a fairly easy audit.

2 Likes

Sonia-Chen #133 July 24, 2019, 3:12am

Great link! **@shemnon** posted another one in gitter that is worthwhile reading: Zcash summary of the last 6 months making sense of ProgPoW - solardiz did an excellent job.

Issue: Design and/or help review new PoW scheme

opened by **solardiz** on **2018-05-17**
closed by **solardiz** on **2019-07-23**

```
I am creating this pre-proposal primarily to get something in by the
deadline, without being sure whether this proposals/grants mechanism
is...
```

full-submission grant-winner invited-full proof-of-work

Sonia-Chen #134 July 24, 2019, 4:19am

@gcolvin

Let's take a moment. You commented publicly, several times, that Linzhi is "not to be believed because if what they say is true they would just go and do it and take the money".

In the nicest words, that is a condescending argument.

Are you implying that everyone is like this? How do I know you are not being paid under the table? In our interesting crypto space, some people try to define "rational" as equal to "corruptible". I totally disagree.

This kind of logic breaks all assumptions FOSS culture and crypto are built upon these last decades.
I understand the difficulty of having a discourse over issues that are partially or largely intransparent, such as hardware.
We have a long list of people that are free to apologize for all the nasty things they said about us in

recent months. Luckily we made lots of new friends also.
I fully expect you to take back the “if what they say is true they would just take the money” comment one day.

Kristy sent out her minions to offer us up to 75 mio USD to participate in her scheme, we slammed the door on them.
You would have done the same.

I stand by everything me and my friends have contributed to the ProgPoW discourse since January, 100%. Some of it is a painful read, because the underlying issue is painful. We are at the beginning, because the points we made, technical and economical/business (the attack vector), have a basis and will show their true face over time.

Humans are not very good at dealing with high complexity. So our brain uses a trick: simplification. Simplification happens unconsciously, one barely notices it. Simplification has one disadvantage: It doesn’t create a closed and consistent logical structure.
Then things become complicated again and the brain tries to disregard or treat things categorically, to reduce dissonance.
If you use simplification consciously and controlled, it’s abstraction.
This is the key ability that is lacking in the discussion, and most importantly the decision making process.
Everything is discussed momentarily. What’s lacking are deeper, long-term and strategic thoughts that are then upheld.

> Secure, proof-of-work, public blockchains are, and will always be, under constant social attack.
> **https://etherplan.com/2019/05/17/ethereum-classic-and-the-permissionless-fallacy/7584/**

Sonia-Chen #135 July 28, 2019, 5:08am

Relevant:
https://www.globenewswire.com/news-release/2019/07/25/1888023/0/en/Squire-Mining-Announces-Appointment-of-Kevin-Turner-to-Advisory-Board.html
Message me if you don’t understand how this relates to ProgPoW or Ethereum.

[edit, for people glancing over this thread: News says boss of EIP-1057 author Kristy now sits on a board of megaminer Squire Mining together with Dr. Craig Wright, who Vitalik called a fraud which Vitalik and others are now being sued for. 🤔]

@OhGodAGirl relax, the truth will come out. Happy writing.
Wish everyone a relaxing Sunday.

Sonia-Chen #140 August 4, 2019, 8:02am

> [typical Kristy way of saying hi]

Good morning Kristy. **@MrAndrewAu** **@OhGodAGirl** **@epic.henry**

The kind of attack ProgPoW is pulling off is anticipated, and will repeat in the future. It's too logical not to try. Make a list of possible motivations for a PoW change, and expect someone to start with the easiest and most profitable ones, the low hanging fruits.

We talk about ProgPoW - **Programmatic Proof-of-Work**.
Programmatic means 'according to a program'. The rarely used 'programmatic' is then substituted by people for the more common 'programmable'. Other confusing terms such as dynamic and random are mixed in.

How can a PoW algo be programmable when it always needs to be verifiable?
PoW is work that someone else can verify, so it cannot be programmable and will always fully derive from a seed, with a series of 100% predictable and repeatable steps. No matter which linguistic trickery someone may be trying to sell the story.

Real innovation in PoW would allow user defined programs to be passed to the PoW algorithm, which would then need to be stored alongside the PoW result, and clients would need to construct a zero-knowledge proof to check that the program was fully executed (limiting CPU time).

None of such real innovation is in ProgPoW, because all it is is superficial pseudo-technology trying to coverup a corporate scheme (follow the links, DYOR).
We can do better, and we will never loose our optimism.

Sonia-Chen #141 August 10, 2019, 10:27pm

> OhGodAGirl:
>
> if the best criticism that can come from it is my involvement, this will be a fairly easy audit.

Noted. You really think people are dumb.
Let's double down, your company is making news again so this needs to be added to the thread:

https://www.globenewswire.com/news-release/2019/08/07/1898434/0/en/Squire-Enters-Into-Development-Agreement-With-nChain.html
I won't paraphrase, at this point it's obvious what's happening. The only thing we will most likely never see are the ProgPoW-related agreements between Nvidia and Core Scientific, and Core Scientific and Squire/nChain. If anyone wants to leak them, DM me.

@OhGodAGirl That should be easy to denounce Craig Wright as a fraud.

How many TH Ethash does Squire/Core Scientific control today, how much will they benefit from ProgPoW? You can ask the CTO right here, she will know and she's oh so trustworthy 🤣
I hope we don't see Ethereum in Coingeek conferences ever.
For Kristy and her sockpuppets (Amel, Jean Cyr, Epic Henry, Teddy Ghannam, Jon Stevens, more created as needed - Andrew Au, Sarah Osbourne, …), what remains is this:

Zero facts, a lot of emotions - but what is the agenda? DYOR

kotarius #146 August 15, 2019, 7:18am

> OhGodAGirl:
>
> Everytime you attack myself, you strengthen ProgPoW and its merits - because if the best criticism that can come from it is my involvement, this will be a fairly easy audit.

I can't speak for Sonia, but every time I publicly draw attention to your less-than-stellar 2-year tenure in the crypto space (DYOR research, Kristy did not exist before December 2017), I am met with boat-loads of new business opportunities stemming from others you've fucked over in this space. I can honestly say that my professional career has benefited tremendously from calling you out with regards to your previous scams.

https://bitcointalk.org/index.php?topic=5134170.0

blahblahblah1 #21 August 17, 2019, 6:52am

Why is a controversial change being shoved through without awareness of the community? Why does **@OhGodAGirl** have so much sway over the governance process?

shemnon #22 August 17, 2019, 9:27pm

"Without awareness of the community?" That is an assertion the evidence does not support.

There were two twitter polls, a carbon vote, a tennagraph vote (both coin and gas weighted), and a miner vote. All of which came back in varying degrees of yes to strongly yes. Is there some community we that should be polled for sentiment that those would not have reached?

blahblahblah1 #23 August 18, 2019, 7:53am

"and a miner vote" Wait, the people who stand to benefit from rigging out their competition are in favor of it? Ya don't say!

"Is there some community we that should be polled for sentiment that those would not have reached?" Yes, the vast majority of investors who don't bother to take part in your tiny, non-representative, socially engineered votes specifically designed to create a false sense support for something no one wants. It's a controversial change being pushed through by a hijacked governance process. If this goes through it means that Ethereum has been officially hijacked.

fubuloubu #24 August 18, 2019, 5:04pm

She, like many other authors of EIP proposals, created a proposal with a reference implementation and went through the process of gaining support by talking about the issue on All Core Dev calls. The client developers all decided there was sufficient technical benefits to implementing the proposals, so the client developers integrated the change. There was significant benchmarking and testing done over the past year since the proposal was created, and an audit is currently in process, the end result of which will hopefully show the algorithm is technically sound and meets it's intended goals (to the best abilities of the auditors).

No where in this was there a deviation from the governance process, which means no "hijacking" occured. Please note that while it is often helpful to the developers to gauge sentiment of the community in this process to inform their decision to implement, it is ultimately their own decision of what work should be integrated. ProgPoW seems to have sufficient amount of community support where it has made it to this stage. At the end of the day, the full nodes govern the rules of the network, the developers only give them the tools to do so.

You may vehemently disagree with that conclusion, and you are free to voice that disagreement. Ultimately, a decision will be made if/when a fork should be proposed, which I believe will *only* contain ProgPoW. I would actually be most in favor of a soft fork approach (with a threshold of over 90%), as that allows the community to expressly show it's final opinion through the number of full node clients who enable this change, which is the most "democratic" option we have available to us in a decentralized system with no identity layer. If it worked for Bitcoin, it should work for us.

Sonia-Chen #25 August 18, 2019, 9:28pm

@fubuloubu
wow your post was so amazing, it motivated me to reply:

> She, like many other authors of EIP proposals

The author of EIP 1057 is a close business partner of Calvin Ayre and Craig Wright. Needless to point to her bitcointalk trust page and many other pages, it's all fitting.
(there are plenty of links in this other thread, I won't post them again. DYOR)
https://ethereum-magicians.org/t/progpow-audit-delay-issue/3309

> talking about the issue on All Core Dev calls

Together with two anonymous people (Mr. Def and Mr. Else). The naivety of the core devs to not even check that, let alone question any of the narratives brought forward, will remain as a lesson how not to do it.

> The client developers all decided there was sufficient technical benefits

That says a lot about their understanding of both ASICs and mining economics. The hardware audit will show (actually several independent audits have shown already), that ProgPoW's promised "asic resistance", lately framed as "closing the efficiency gap" does not exist.

> There was significant benchmarking and testing done over the past year

All of it nice Nvidia marketing material. They didn't even bother to change their bar charts to make them look more "community like". It was enough to make the core devs believe, so well done!

> and an audit is currently in process, the end result of which will hopefully show the algorithm is technically sound and meets it's intended goals

Of course not. We can expect the software audit to mostly look at the algorithm as a cryptographic algorithm, as we have seen with the four RandomX audits.
The PoW-part of the algorithm is a hardware assessment. The hardware audit will show that the promised benefits ("1.2x instead of 2x") do not exist.
The one effect ProgPoW has is from the PoW change itself, that's very disruptive and benefits the large farm of the EIP 1057 author whose contracts with Nvidia we don't know. A PoW change is like an ICO, it's fitting that the people behind ProgPoW have a deep ICO history.

> which means no "hijacking" occured.

It was hijacked from the beginning, and persists until today. The motivation behind EIP-1057 is entirely different from what is stated in the EIP text. Welcome to the real world.

> ProgPoW seems to have sufficient amount of community support

What was actually measured in these votes - hashrate, distinct human beings, mining pools, capital? Since the votes came out largely in favor of ProgPoW, what does this mean about centralization? Wouldn't a large majority, in some cases 100%, say something about the state of centralization?

On the day this proposal was made (2018-05-03), Ethash hashrate was 265.97 TH at a profitability of 6.22 US cents/MH/day. Happy old days!
Today, Ethash hashrate is 178.83 TH at a profitability of 1.51 US cents/MH/day. (numbers from **bitinfocharts.com**)
There probably were never more than a few TH of ASICs on Ethash, and Ethash ASICs haven't been on sale for a year. I did math to walk through mining economics in the other thread.

So if ASICs played a small role in Ethash 15 months ago when EIP 1057 was launched, and are not economical to sell since then, why is there continued pressure to switch to ProgPoW urgently?
You cannot think about this hard enough.

Will ProgPoW accelerate centralization?

> I would actually be most in favor of a soft fork approach (with a threshold of over 90%), as that allows the community to expressly show it's final opinion through the number of full node clients who enable this change, which is the most "democratic" option we have available to us in a decentralized system with no identity layer

It would be far healthier for the Ethereum ecosystem to uncover and investigate the background story of ProgPoW:

- Why is the “anti-asic” effect less than promised, if supposedly so many “experts” from Nvidia and AMD were involved. Is it an error in judgment, or is there some other story going on?
- Who are Mr. Def and Mr. Else? If they are Nvidia employees and Nvidia was trying to exclude Bitmain, Samsung and others, what else does Nvidia plan?
- Are Mr. Def and Mr. Else engineers, or marketing people?
- Is it acceptable that fully anonymous people participate in major Ethereum decision making processes?
- If the authors of ProgPoW are anonymous, what does this mean in terms of copyright or patent claims?
- Why is the EIP-1057 author working with Calvin Ayre and Craig Wright, and what does this mean for ProgPoW?
- How many TH Ethash does Squire/Core Scientific control today?
- What are the contracts between Nvidia and the company of the EIP 1057 author, as well as Squire (Calvin Ayre/Craig Wright company)?
- Is it possible that Nvidia sells chips at a discount to the EIP 1057 author in return for excluding competitors?
- Does ProgPoW help with decentralization, or help with centralization?

I think the attack from Nvidia and partners (Core Scientific, Squire) is sophisticated, the largest corporate attack on a coin ever.
The Ethereum Foundation needs support in that they managed to at least put order to the process by bringing in independent auditors for both software and hardware.
Too bad noone can audit the contracts of the company of the EIP 1057 author…

The EIP-1057 author is already trying to discredit the hardware auditor (“I do have some concerns that someone who has not built crossbars for GPUs will be doing a hardware audit on the ability to build a crossbar in an ASIC - but given the lack of choice due to CoI this seems fitting.”), but hey, she is a hard worker.

Looking forward to the audits! Hope Least Authority and Bob Rao crush some of that dark corporate stuff.

Sonia-Chen #28 August 19, 2019, 4:25pm

@fubuloubu

> I don’t see how the results would be suspect, but it may be underwhelming.
> … he might miss some nuanced thing that only those with deep expertise might know

You cannot compare what an honest person and a liar are saying side-by-side, and learn anything from that. You first need to identify the liar.

The discovery, and innovation, of ProgPoW was that if most of the audience relies on a very small amount of a posteriori knowledge in some field (here: PoW and ASICs), while for the most part

having to rely on a priori knowledge, then the best strategy is to aggressively promote one's own credibility and experience, while discrediting everyone else.
This sets the stage for the successful adoption of a hidden agenda, because a posteriori knowledge is the only way to reliably identify the liar.

The key mechanism of the attack is neither identified nor understood, and there seems to be limited motivation to change that so far. Maybe the audits will re-energize such efforts.
Instead, core devs believe a form of technocracy where numbers, ideas and codes are pushed through some process will lead to the best possible result.

ProgPoW is successful these last 15 months not because of their technology, which sucks, plain and simple.
They are successful because they have managed to draw attention away from things that are of high relevance to most people, and towards things that are of low relevance to most people.

Sonia-Chen #31 August 20, 2019, 6:18am

@fubuloubu

Absolutely breadthtaking, yes? The attack continues right under our eyes.

Sonia-Chen #33 August 21, 2019, 5:26am

Yay! Relax Kristy, ha ha.

I think Bryant meant the free advice from me, not the one he took from you, Mr. Def, Mr. Else, and so on - for over a year.
That is very hard for anyone to go back and realize they have been played since the beginning.

BTW I would totally choose to ignore Epic Anything no matter what they said, because as we are saying from the beginning - who actually reads spam?

ProgPoW author Kristy-Leigh Minehan is CTO of Calvin Ayre and Craig Wright's hosting company Core Scientific.
https://globenewswire.com/news-release/2019/08/07/1898434/0/en/Squire-Enters-Into-Development-Agreement-With-nChain.html
https://globenewswire.com/news-release/2019/07/25/1888023/0/en/Squire-Mining-Announces-Appointment-of-Kevin-Turner-to-Advisory-Board.html

Squire Mining Signs LOI with Core Scientific in US$6.37 Million Deal | INN

The agreement will bring together Core Scientific's AI-driven infrastructure and Squire's cloud computing units.

https://www.corescientific.com/team

The CTO of Craig Wright's hosting company is "improving" Ethereum? ha ha. yes. We can see that!

Sonia-Chen #147 August 26, 2019, 12:52am

@kotarius Oh sure, same here.

Randomshortdude has been digging out some spectacular stuff, that should be added to this thread for people who care to do homework.

> **r/ethereum - ProgPow Tied to a String of Investment Fraud**
>
> 13 votes and 92 comments so far on Reddit

On a lighter note, Kristy's been working so hard this past year, the auditors will turn around every line of her 50 lines of code many times, so in the meantime we can think about the truth behind ASICs. Straight from the source, the 25 ASIC truths!

ASICs are specialized devices
ASICs are single-purpose devices
ASICs are fixed-function devices
ASICs lead to centralization
ASICs are scarce, inaccessible, subject to tariffs
ASICs are from China
ASICs are at war with the home miner
ASICs create backdoors
ASICs are biased against evolution
ASICs are chasing one incentive, and that incentive is to make money
ASICs are a malignant tumor for the network, rather than an antibody
ASICs are locked into a dead-end route
ASICs are desperately focused on finding a reason for this hardware to exist
ASICs let the tail wag the dog
ASICs make decentralization highly implausible, if not improbable
ASICs want to attack the networks they secure
ASICs are nomadic
ASICs gamed the mining metric in a way that encourages everyone to buy more
ASICs attack without rhyme or reason
ASICs will go out of their way to protect their investment, whatever the cost
ASICs have the flavor of the lemon tart almost
ASICs are the king
ASICs are a cancerous element extending to blogs and forums where they spread misinformation and fearmonger to hide their motives and damage they do
ASICs attacks are constant and pervasive
ASICs have guided the evolution of Bitcoin into a version of the traditional banking system, where they now hold all the keys

🤣

Sonia-Chen #150 September 5, 2019, 9:29pm

@souptacular emailing **progpow-audit@leastauthority.com** didn't work for me (delivery failure, you may not have permission, may need to join, group may not be open to posting).

Referring to the initial audit, dated 16 August 2019

Key Omissions

1. Most of the Areas of Concern (p.3) not addressed:

Security of the algorithm: *"security" not defined*.
Cost of a 51% attack: *No reasonable calculation attempted*.
Other security risks from a change of PoW: *Not attempted*.
Impact on "fair mining" and uneven distribution: *No calculation*.
Possible changes to hash power and miner balance: *No data, no calculations*.
Other potential effects impacting the ecosystem: *Not attempted*.

2. No measurement for "centralization" proposed or attempted

How centralized is the 170 TH network today, how could one model the effect of ProgPoW towards centralization?

3. Background and motivation of ProgPoW proponents not considered

The ProgPoW author is CTO of Craig Wright's hosting company Core Scientific. Together with two anonymous co-authors.
The identities and motivations of the ProgPoW team remain a mystery and were left out of the audit.
Serious consideration of Core Scientific's and Nvidia's business interests with regards to ProgPoW are warranted to understand security implications.

4. No definition of "attack" proposed

PoW is a control vector for the entire decentralized network.
Measurement of real-world centralization is a prerequisite for the mitigation of attacks. "Attack" needs to be defined. An optimization of the PoW algorithm, sold in an ASIC, is not an attack in our opinion. "Attack" is not when someone openly plays by the rules. "Attacks" come from behind. A trojan horse is an attack.

5. Economies of Scale

The audit does not clarify whether economies of scale are seen as positive or negative factors towards decentralization.

Details

1. Random & Pseudo-Random

p.5 “*Our review and analysis results in our agreement that the KISS random number generator is sufficient to make the sequence of math in the main loop unpredictable*”

KISS is a pseudo-randon number generator. The difference between random and pseudo-random is fundamental. The audit uses the term “random math” 8 times. One would hope that everyone understands that this is pseudo-random and thus predictable.
If it was unpredictable as the audit states, it would be unverifiable.
With traditional PoW one needs to remember that no matter which calculation the algorithm performs, it needs to be verifiable, meaning it needs to derive from a seed.

2. Keccak optimized for 32-bit

p.4 “*We examined the hash function, a non-standard instance of the Keccak function that is optimized for 32-bit architectures*”

The audit fails to ask the question why the change to the non-standard 32-bit optimization may have been made.
With sufficient and actual study of the business interests of the parties involved and their potential agendas, we came to the conclusion that 32-bit multiplication was pushed under the pretense of it being inefficient on both Nvidia and AMD but that turns out to be a lie as on Nvidia it was only inefficient on Pascal. The algorithm is tuned to still let Pascal utilize full memory bandwidth due to simply sheer compute capacity difference coming partially from higher die size which is why comparing GPUs based on price is being pushed as of late. It’s not a secret that 4xx & 5xx series AMD GPUs are not high-end but because ProgPoW’s compute to memory bandwidth ratio is tuned to match Nvidia GPUs, AMD GPUs are not utilized to their fullest, most importantly losing the full memory bandwidth utilization which is the very basic foundation of the Ethash algorithm.

3. Limiting Efficiency Gains
p.7 “*the circumstances in ProgPoW are much more favorable due to the additional random math core*”
p.7 “*the random math core likely prohibits the build of a light-evaluation based ASIC*”
p.8 “*the additional use of random math sequences extends the ASIC resistance of Ethash substantially*”

These statements support the key ProgPoW claim (from the EIP) that ProgPoW results in “minimal, roughly 1.1-1.2x, efficiency gains. This is much less than the 2x for Ethash”.

Both the EIP claim as well as the auditor’s confirmation of that claim are wrong. The pseudo-random math core increases the efficiency gains an ASIC can achieve, because an ASIC can implement the math logic more efficiently than a GPU.

4. Sarah Osbourne
p.17 “*Sarah Osbourne Response to the Linzhi ASIC post*”

The audit cites the Sarah Osbourne response in the rather short list of third party resources consulted for the audit.
How can an account that was created the day before the post, and has since only posted that one response purporting to possess highly specific knowledge about ProgPoW and GPU/ASIC design, not be further scrutinized?
Who is “Sarah Osbourne”, who pays her/him/them, what is the agenda?

If the people that are behind “Sarah Osbourne” are in fact Nvidia or Core Scientific employees, writing under pseudonym has the pleasant side-effect of not even affecting their reputation, shall the response be proven wrong. We would just prove “Sarah Osbourne” wrong, an anonymous one-post-only person from the Internet. Then the next anonymous person would show up with new claims.

What is happening here is FUD marketing. The Sarah Osbourne response is the “D” in FUD - doubt. It’s written to cast doubt over the Linzhi post, and does so effectively.
We have removed the intentionally deceptive Sarah Osbourne post from under our article.
Trust Sarah Osbourne or trust Linzhi or trust neither of us and verify yourself.

5. Asymmetry of Proof and Verification Workloads
p.10 “*it would change the amount of cycles required for verification*”

The asymmetry in workload between proof and verification is a key attribute of PoW. The audit fails to show to which degree ProgPoW worsens the asymmetry, which impact this has on mobile clients and how one could model the impact of this on the decentralization of the network.

6. Programmatic and Programmable
p.8 “*The rationale of extending Ethash into a programmable PoW, by integrating a random math core*”

ProgPoW is not “programmable” as in the typical meaning of that word among software developers. It cannot be programmable because it would then be unverifiable.
A real programmable PoW would need to store the program along with the proof, and define a system of verifying that the program was executed in less time than the actual execution, similar to a zk-proof.
ProgPoW adds a convoluted pseudo-random math logic to Ethash.

---

chfast #151 September 6, 2019, 10:47am

> Sonia-Chen:
>
> **2. Keccak optimized for 32-bit**
>
> p.4 “ *We examined the hash function, a non-standard instance of the Keccak function that is optimized for 32-bit architectures* ”
>
> The audit fails to ask the question why the change to the non-standard 32-bit optimization may have been made.
> With sufficient and actual study of the business interests of the parties involved and their potential agendas, we came to the conclusion that 32-bit multiplication was pushed under the pretense of it being inefficient on both Nvidia and AMD but that turns out to be a lie as on Nvidia it was only inefficient on Pascal.

Keccak does not use multiplication at all.

4 Likes

Sonia-Chen #152 September 6, 2019, 11:03am

Thanks for reading, and you are right! I saw “32-bit” and jumped to a conclusion. The gems are hidden. Thanks for the correction!

Sonia-Chen #153 September 6, 2019, 9:13pm

@chfast

Apologies it took me a moment but I wanted to get permission from hyc and sech1 to quote them here.
What do you think are the reasons for choosing int32 math?

hyc and sech1 are key contributors to Monero’s RandomX PoW algo, with deep knowledge around ASIC Resistance, or rather chip economics and performance. Both RandomX and the people behind it are highly recommended.
The following is an excerpt from the #monero-pow channel on Freenode today:

> **< hyc >**
> the fact that progpow only uses integer math leaves the door wide open for ASIC optimization.
> GPUs are loaded with floating point math units
> none of which would be needed in an eth/progpow ASIC
> **IMO progpow will widen the gap btw ASICs and GPUs, with GPUs losing out**

> **< sech1>**
> yes, I have the same feeling. While with ETH you could underclock/undervolt GPU core and have most power used on memory, it’s not the case with ProgPoW.
> ASIC could save on core power, but it’s a smaller part of GPU power usage on ETH
> but it’s different in ProgPoW
> and their reasoning for not using FP32 is just false
> RandomX has no problems with FP

> **< linzhi-sonia>**
> hyc: sech1: do you mind if I post your statements (the last few lines) about progpow in an eth/progpow thread? (attributing to hyc and sech1)?

> **< sech1>**
> I stand by my words
> yes, I think ProgPoW makes it worse
> What I would do with progpow is I’d minimize computations (even less than in Ethash) while adding randomness and FP32
> same size of mix state, same number of parallel lanes, but much less computations and FP32 instead of int would be perfect for progpow
> that would make ASIC chips bigger anyway but potential advantage smaller because GPU core would run at minimal clocks and voltage

> and then maximize amount of calculations for these clocks and voltage to still have >90% of memory bandwidth used
> so they kind of did everything right except they made progpow more power hungry
> should’ve been the other way
> and not using FP32 is a big mistake
> even with existing progpow, simply tweaking parameters until it’s less power hungry than ETHash will reduce ASIC advantage for real, by all metrics
> yeah, now that I think of it more
> progpow team did everything right except for not using the most efficient GPU clock/voltage when tweaking parameters
> they probably ran everything at stock
> which is stupid if you ask any miner

> **< hyc>**
> linzhi-sonia: sure, fine to quote me. this is a public channel

---