Linzhi Semiconductors

Linzhi Working Papers
No 7

Does the Origin of Open-Source Code Matter?

by Sonia Chen

February 2019

Keywords: LWP7, Open-Source, Principles, Scrutiny, Accountability, Scam, Fraud, Trust, Anonymity, Ethereum

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

reddit

ProgPoW: Does the origin of opensource code matter?

11 points | 48 comments | 14 days ago ago by **LinzhiOfficial** from ethereum

**** Update Feb 14, 11:30 GMT: Maybe the answer is the origin of open source code does not matter, but the energy flow matters. How do we go from opensource to openenergy, and slightly separate but related can we define computer rights? People who accept closedenergy code have to trust the author, and we see in this post how vicious some authors may dodge questions, for whatever reason. People who insist on openenergy code don't need to trust the author, but need to define what is highquality openenergy code. ****

**** Update Feb 14, 7:50 GMT: Our account remains banned, thanks everyone for the great discussion. ****

**** Update Feb 13, 20:05 GMT: Well due to account ban we cannot reply anymore. Or remove spam. Our Wikipedia page also got vandalized ("company does not exist"). Free speech in the western hemisphere. Some people seem to care a lot about the origin of opensource code. We are powered by happiness. ****

**** Update Feb 13, 19:15 GMT: Someone had this post removed from the subreddit and the posting account banned. Apologies to commenters that we cannot reply anymore. Please help Ethereum, do your own research. ****

[Disclaimer: We work on Ethash ASICs and would benefit from ETH remaining with Ethash longer]
Continuing a conversation with DaftWullie from gitter, about whether the origin of the ProgPoW sources matters or not:

Anonymous and pseudonymous contributions in opensource used to be exceedingly rare, and were never discussed to any serious degree. Opensource principles relied on responsibility, pride, transparency. Linux kernel contributions without disclosure of employment status would have been mostly unthinkable.

That was until **Satoshi had the mercurial idea of releasing code into the world that was not tracable back to anyone**, from day one. Satoshi gifted us with this, but he also caused new problems. What if Satoshi had a secret deal with the US Federal Reserve who is today in possession of his 1 million BTC?

https://www.masteroffinance.org/10mostoutrageousstockmarketscammers/

If you read over these stories, you notice they all run for many years, a lifetime even. Crypto has created many getrichquick millionaires. Why would you think crypto couldn't also create swindlers that made it into this list?

Anyone is free to believe KristyLeigh Minehan's [*] stories about ifdefelse and ProgPoW, in the same way that **we have to believe Satoshi had no secret deal with the US Fed**.
[* KristyLeigh Minehan is the main proponent and only currently known public face of ProgPoW]

Some of us like to say code is law, or code is money. We like to think of ourselves as "better" than the traditional banks and state institutions. So "code is law" means that criminals can write the laws? Code is money means swindlers can directly mess with the creation of money now?

When you want to become board member of a traditional bank, you will be background checked. We laugh about this because we are better?KristyLeigh Minehan would not stand the chance of being considered, given all suspicious evidence out there.

Let's start somewhere. She says about herself
https://www.corescientific.com/team

"has been writing optimized cryptocurrency miners since 2010"

Would like to see proof. github? sources?

"In 2013, founded a company that became the **leading provider of hardware optimizations for GPUs** and ASICs".

Leading provider of hardware optimizations for GPUs? Sorry I may be old fashioned but that leads to dozens of questions in my mind, if that is the same person who then comes forward saying ProgPOW is an attempt to bring mining back to GPUs and make it fair again.

"founded Mineority Group, achieved over 100M annual recurring revenue"

That was the company that went bankrupt? KristyLeigh Minehan herself yesterday said "a host of people think she embezzled money" but "they don't understand business". hmm.
https://www.reddit.com/r/gpumining/comments/a27lhb/so_ohgodagirl_and_the

Why is an exemployee of her saying he or she "**got a rare insight into the evolution of ICO and cloud mining scams**" ?

https://www.glassdoor.de/%C3%9Cberblick/ArbeitbeiTheMineority EI_IE2404190.11,24.htm

There is so much more, some publicly available to the openminded, and a lot more known and shared privately.
"NO ONE CARES" anyway, right?
If the coin price recovers there will be so much money coming out of Kristy Leigh Minehan's deals that it will be impossible to hide. Nvidia shareholder lawsuits will come, her friends at Nvidia will loose their jobs, Core Scientific can scrap their IPO plans. Ethereum will be impaired for good.

What is the identity of Mr Def and Mr Else? Another two Satoshis...
We do have the voices of two of them in the developer call recordings on Youtube, a starting point.

If it turns out ProgPoW was written by Craig Wright, would you care?
If it was written by Linzhi, a Shenzhen ASIC maker, would that be OK too?

Any ideas how to back out of this mess?

KristyLeigh Minehan could resign from Core Scientific, come clean to the Ethereum Foundation, who could get a **written guarantee from Nvidia to not favor selected miners with secret optimizations or special chip deals, and only sell to all miners on an egalitarian basis through distributors**. The Ethereum Foundation might be able to get such Nvidia assurance because of the danger of shareholder lawsuits.

Someone will want to take some responsibility BEFORE it's a big story.

[Disclaimer: We work on Ethash ASICs and would benefit from ETH remaining with Ethash longer]

---

cosminstefane | 14 points written 14 days ago ago

Hi Sonia,

Because you were left without **TECHNICAL** arguments on gitter, you also engage now in something personal against somebody.

r/EthereumCatHerders was asked already to check at least the technical aspects of PorgPow. /u/poojaranjan19

How about leaving out the drama and focus on technical or at least let us do that?

Personally myself I have started testing on different VGA's.

I don't care who Satoshi is, I don't care who IfDefElse is if their algo is good.

Maybe they wanted to stay anonymous in order to protect themselves from manufacturers of ASICs.

In this crypto world you never know what could happen.

Considering what happened to Kristy with all the attacks to her personally, including this one (even if it's real, I don't care) maybe the others wanted protection against such kind of actions.

> **Crypto_Economist42** | 1 point written 13 days ago ago
> Of course it does not matter the code is open source anyone can read it and then debate it.
>
> If you have conspiracy theories about collusion with Nvidia for secret speedup then show proof! Not just make up stories.
>
> > **LinzhiOfficial** | 0 points written 14 days ago ago
> > Thanks for replying. So you think the origin doesn't matter, that is a very valid viewpoint and was the point of the reddit.
> > I think we have no answer to this right now, time will tell. Basically you are saying whoever writes the codes doesn't matter, as long as the community supports it.
> >
> > > **WinEpic** | 4 points written 14 days ago ago
> > > Well, if code is published, its author becomes irrelevant. A quicksort written by a serial killer is not any different from a quicksort written by

a Linux kernel developer if many people have reviewed the code and found it to be equally as good.

The origin of software matters when it’s closed source, because then the only real way to know the intention of the programmer is what they are claiming. If it’s open source, we can figure out what the developer intends by reading the code, and who they are or what they claim takes a backseat to what the code says.

> **McDongger** | 0 points written 14 days ago ago
> Look at the parity multi sig bug. Honest mistakes were made, nobody detected them and as a result the ecosystem suffered.
>
> Do i trust parity to act in the interest of Ethereums ecosystem? YES!
>
> Do i trust anonymized developers to act in the interest of of Ethereums ecosystem? Well, no I can’t, because I know nothig about them.
>
> Audits can only do so much, i very much prefer the added “security layer” of aligned incentives.
>
> > **WinEpic** | 3 points written 14 days ago ago
> > The counterpoint is that audits, especially community audits, get more lax once the entity publishing the code becomes more trusted. When we distrust the code’s publisher, we tend to scrutinize everything and this might lead to things being found that wouldn’t be otherwise.
> >
> > Your point is very valid though knowing that the person writing code isn’t trying to get to your money is definitely reassuring.

Xazax310 | 7 points written 14 days ago ago
First, satoshi's wallet is closely watched by many cryptoenthuasists. Even a single microtrasaction would bring massive attention. Anything with him including craigwright claims are throughly mistrusted. For all we know Satoshi could be a team of people not just one person.

Nvidia and AMD have both publicly stated, they don't care about cryptocurrency and the goings on. They both reaped the rewards in 2017/2018, however Nvidia suffered from overproduction of 1000 series and releasing the 2000 series which hurt them far more than AMD who, still is limping on the RX 500 series for midrange.

> **written guarantee from Nvidia to not favor selected miners with secret optimizations or special chip deals, and only sell to all miners on an egalitarian basis through distributors**.

There extremely small teams I'm sure on both sides involved with blockchains, none care about making any one crypto GPUmineable. Your asking for the

impossible and improbable. Nvidia isn't going to release some statement on ProgPoW.

Nvidia does well in ProgPoW so we should be careful about Ohgodagirl and IfdefElse "backdoor deals"

That's a totally a Ad Hominem Fallacy. So can we get the same thing for X16R? Zhash? GRIN? Their teams have backdoor deals with massive nvidia mining farms? Nvidia dominates many algorithms already because of there much more efficient architecture and CUDA implementation in lowlevel software rather than using OPENCL.

There's thousands of AMD farms, far more than Nvidia's. Going off ETHOS own page RX470's are top cards used, then RX480s, and lower on the rung is the P106/104/P102 cards. I would say AMD OEMs were giving the special treatment to many larger farms rather than individual miners during the lowstock period. Nvidia was extremely late to that game and barely reaped any rewards. Changing the algorithm to ProgPoW isn't magically going to make Nvidia billions of dollars because of sales of GPUs. All it's going to do right now is make GPUmining for Ethereum viable for another year or two... at best.

IMHO GRIN would be a better focus for your attention to create and ASIC for. GRIN is stated to become an ASICAlgorithm and throwing off GPU miners. It's ironically an Nvidia dominated Algorithm right now btw.

I do have an honest question.

Theoretically, because Ethereum is built in an Difficulty bomb/iceage and say we don't move to ProgPoW. what then? How are ASIC farms going to stay profitable in that timeperiod? When the difficulty ticks slowly upwards. How could you sell ASICs then? Who would buy? There's no chances of quick ROIs on Ethereum. It's not built like other cryptos.

ASICs then would flood other Ethhash networks until the profitability of them is barely anything. Most would be sold for nil or dumped in landfills because they are not useful for anything else. The idea that you're going to walk graciously away is stupid. You're investing millions into manufacture and engineering these ASICs. You can recoup maybe your initial investment selling/selfish mining, but in one or two years its going to be basically be nothing. ASICs aren't a sustainable model for Ethereum and Ethhash.

> **LinzhiOfficial** | 0 points written 14 days ago ago
>
> Thanks for the dialogue. This post is about whether the origin of opensource codes matter. Do you think it matters or not?
>
> About the ASICs, we invest in chip technology. Our chip technology can be applied to many problems. We are actively working on many other blockchainrelated ASIC ideas STORK provers, signing or verifying accelerators, block speed accelerators, ETH gas turbos, etc.

Any coin community can choose to reward whatever performance they like. Right now ETH rewards Ethash, maybe in the future the ETH community rewards ProgPoW (for which we could also make a chip). Our continuity is in our chip technology, not in the software side. The software is always open source.

For example we think it would be an interesting idea to get blockchain data into the PoW algo. For the chip that would be very interesting, for verification it would be a problem. Those are the things we work on. Thanks for asking!

> **Xazax310** | 3 points written 14 days ago ago
> If it was about opensourced code.. then you may want to make a better argument it's not quite how i read that, but...
>
> I'm not a developer, just a lowlevel hardware guy, GPUMiner, so from what I understand if the code is open sourced then that means it can be fully viewed, nothing is hidden or closed off. If Ohgodagirl/IfdefElse team did not release ProgPoW as opensourced code then I would agree to your objections, but it is.
>
> Additionally you in a sense lobbied to have the code verified. So guess what Ethereum Developers and foundation are doing? They're auditing ProgPoW. The Catherders are on it. We all just have to await the results.

> **greerso** | 2 points written 14 days ago ago
> ProgPoW is only a small extension of Ethash, when Ethereum adopt the small code tweak, ProgPoW, it will still be Ethash, it'll just be a more efficient PoW algorithm than it already was.
>
> A ProgPoW compatible Ethash would be great for Ethereum and miners that prefer that plugandplay convenience. You cannot make one more than 1.2x more efficient than a GPU with the same memory type and presumably will not be able to make a profit selling them in the short amount of time before PoS.
>
> I also presume that your company will likely not survive the adoption of ProgPoW by Ethereum or you wouldn't be making such public flawed arguments, sometimes outright lies, against it which have already caused irreparable harm to your reputation.
>
> > **LinzhiOfficial** | 1 point written 14 days ago ago
> > Thanks for your feedback. It sounds like you don't believe the origin of opensource code matters. Thanks!

OhGodAGirl | 8 points written 14 days ago ago

You know, normally I wouldn't reply to this, but hey I'm in transit in an airport, it's been a good week, and I'm feeling rather chatty.

I make you a promise, Linzhi: a new world of mining is coming, and you are not a part of it. Unanimously, we stand up as miners and reject toxic manufacturers and toxic culture. We reject the days of fixedfunction hardware locking the network into a few participants. We reject the days of mud slinging, and we unite to create a better culture: the culture Ethereum was built from the ground up on an ecosystem of GPUs. No one is exempt. Everyone can participate.

We reject you, Linzhi.

Every arrow you put into my back is one more that I'm happy to wear as a badge of honour, because for too long, individual miners have not been given a voice in this ecosystem.

You'll silence them no longer.

I'll see you on the battlefield.

Note: If you don't get the sarcasm above, it's not intended for you. The only way I know how to fight silliness is with silliness.

> **McDongger** | 4 points written 14 days ago ago
> Wtf is this?
>
> "A new world is coming" , "battlefield" , "every arrow you put into my back is one more that i'm happy to wear as a badge of honour"
>
> You do realise that PoW is just a gap filler until we reach PoS?
>
> > **akira_fmx** | 1 point written 13 days ago ago
> > It was sarcasm.
> >
> > > **alsomahler** | 1 point written 13 days ago ago
> > > Poe's Law
> > >
> > > > **WikiTextBot** | 1 point written 13 days ago ago
> > > > **Poe's law**
> > > >
> > > > Poe's law is an adage of Internet culture stating that, without a clear indicator of the author's intent, it is impossible to create a parody of extreme views so obviously exaggerated that it cannot be mistaken by some readers for a sincere expression of the parodied views. The original statement, by Nathan Poe, read:
> > > >
> > > > Without a winking smiley or other blatant display of humor, it is utterly impossible to parody a Creationist in such a way that someone won't mistake for the genuine article.
> > > >
> > > > [PM | Exclude me | Exclude from subreddit | FAQ / Information | Source] Downvote to remove | v0.28
> >
> > **qratz** | 1 point written 9 days ago ago
> > Did you not realize replying to a well known scammer and perpetual victim who could not care less about what happens to ETH if it were not for the financing coming from her business partners?

> She is the main reason why people are wary of ProgPOW. She is well known for defrauding people or accusing them of rape if needed, openly boasting about malicious illegal acts yet some dumb asses believe she is totally saving ETH and making GPU mining great again totally for FREE without being prepared with specialized miners despite of working for a company working on exactly that.

lfc052505 | 2 points written 14 days ago ago

Thank you for stating the obvious. I've grown so tired of the passive, pseudoworrying, concerntrolling tone of this team of people who have bet their farms on ASICs. This is a high stakes game and they won't stop either, but thankfully, most people can see right through it.

MoneroCrusher | 1 point written 14 days ago ago

What are the new numbers for RX 570?

> **greerso** | 1 point written 14 days ago ago
>
> Check them yourself with Andrea's ethminer. Anything that anyone else tells you should not be trusted. You can get the miner here https://github.com/andrealanfranchi/ethminer. To benchmark use:
>
> ```
> ethminer.exe -M 300100 -A progpow --diff 5 --HWMON 2
> ```
>
> 300100 is the block that I benchmarked on.
>
> On an RX580 with a stock bios, limited oc/uv (1300core/2000mem), I'm currently getting 13.23MH/s, 135W at wall. This with the AMD OpenCL compiler bug still an issue, once that is fixed will see results in line with ROCm which with same hardware does not have an issue.
>
> Hash rate varies on each block, on a pool mining the testnet, I have seen >13MH/s on some blocks and <12MH/s on others.
>
> > **MoneroCrusher** | 1 point written 14 days ago ago
> >
> > Thanks for the guide. How much do you get with ROCm?
> >
> > > **greerso** | 1 point written 14 days ago ago
> > >
> > > I'll let you know when I've figured out how to benchmark ROCm. My comment on it is based on what an ethminer dev said.

ianmackay00 | 1 point written 14 days ago ago

What kind of elitist reply is this? You can’t “win” this situation by acting like this. Prove yourself or move out of the way.

> **qratz** | 1 point written 9 days ago ago
>
> Why would not she feel elitist. She recently defrauded likely thousands of people and ran away with millions and she is not only not behind bars, a lot of miners are so dumb they believe her being the crypto savior.
>
> The only place she is going to move out from is her current company. Someone will get the good old rape accusation she successfully used in previous companies then will move onto the next startup. If you see B. Kevin Turner being investigated for rape you know what will be up.

qratz | 1 point written 9 days ago ago

Interesting to see you not getting any smarter after all your dumb and illegal acts. I would rather see you wearing the arrow in your back that reads

"KristyLeigh Minehan was let go from Core Scientific after O1A visa fraud investigation". It is still a shame they keep on tarnishing their own name and reputable ones like B. Kevin Turner with lowlife scammers.

Do people really buy your new scam just because you keep on deleting your posts including boasting about working on ASICs before?

LinzhiOfficial | 1 points written 14 days ago ago

Thanks for replying. Since you have a history of deleting all your social media uploads every few months, let me copy this one right away to preserve it. I guess your answer to the question is that you don't think the origin of opensource code matters. Thanks!

OhGodAGirl wrote:

You know, normally I wouldn’t reply to this, but hey I’m in transit in an airport, it’s been a good week, and I’m feeling rather chatty.

I make you a promise, Linzhi: a new world of mining is coming, and you are not a part of it. Unanimously, we stand up as miners and reject toxic manufacturers and toxic culture. We reject the days of fixedfunction hardware locking the network into a few participants. We reject the days of mud slinging, and we unite to create a better culture: the culture Ethereum was built from the ground up on an ecosystem of GPUs. No one is exempt. Everyone can participate.

We reject you, Linzhi.

Every arrow you put into my back is one more that I’m happy to wear as a badge of honour, because for too long, individual miners have not been given a voice in this ecosystem.

You’ll silence them no longer.

I’ll see you on the battlefield.

McDongger | 3 points written 14 days ago ago

Kind of ironic that you deleted your post.

jacksonobrian | 2 points written 14 days ago ago

> Thanks for replying. Since you have a history of deleting all your social media uploads every few months, let me copy this one right away to preserve it. I guess your answer to the question is that you don't think the origin of opensource code matters. Thanks!

tHaNkS FoR RePlYiNg. SiNcE YoU HaVe a hIsToRy oF DeLeTiNg aLl yOuR SoCiAl mEdIa uPlOaDs eVeRy fEw mOnThS, lEt mE CoPy tHiS OnE RiGhT AwAy tO PrEsErVe iT. i gUeSs yOuR AnSwEr tO ThE QuEsTiOn iS ThAt yOu dOn't tHiNk tHe oRiGiN Of oPeNSoUrCe cOdE MaTtErS. tHaNkS!

alsomahler | 3 points written 14 days ago ago

So "code is law" means that criminals can write the laws?

Ah no, that's not what it means to me. Quite the opposite. It means I follow code instead of a reputation. With the DAO fork, most people here also followed code.

Except this time, the code said that there was an irregular state transition. It didn't matter who wrote it, it matter what you followed.

tromp | 4 points written 14 days ago ago

I think this whole argument boils down to two contradictory claims.

Define "Gap" as the efficiency gap that a (reasonably priced, possibly employing HBM) ASIC can achieve over a high end consumer GPU in the next few years.

The claims and their implication are:

1. Gap <= 1.5x , hence progpow adoption guarantees that GPUs remain viable until the switch to PoS.
2. Gap >= 3x, hence replacing ethash by progpow is mostly futile.

Both sides claim to have sufficient ASIC design expertise to support their bound, yet the factor 2 discrepancy is clear. Most of the other people in the discussion lack the expertise to decide which side is right, but seem to have nevertheless made up their mind one way or the other.

All the talk about characters, connections, motives, agendas is just pointless FUD.

2miners | 3 points written 13 days ago ago

You've started with Satoshi. Great. We all don't know if he is the US Federal Reserve or not. However his code was revised many times. Millions of people in the World use Bitcoin. What do you expect? Stop using Bitcoin? Are we all screwed?

Crypto could be anonymous. Why not? If the product works who cares if the creator was an anonymous or a disclosed person? You analyze the risks and either accept them and use the product or do not use it.

We do not know if KristyLeigh is paid by NVIDIA or AMD. However if her code is good we should use it and keep ASIC's aboard. We'll tell you why:

1. GPU is real decentralization. GPU's are sold all over the World.
2. NVIDIA and AMD are wellknown companies with total market capitalization over $100 billion. Their capitalization is + same as the entire crypto market. Can we trust this companies? Can we assume they have no backdoors? Wow! Yes. We can. Their reputation costs so much. What is more if NVIDIA and AMD are interested in crypto market and paid KristyLeigh for her work we must say we are f*cking doing great! (the moon is near lol).
3. You've told that the first batch of your ASIC's pays out RND. What then? You could easily close the company. Change the name and start over.
4. ASIC manufacturers do everything ONLY for the MONEY. They have no other ideas. Why should we feed them?
5. ASIC manufacturers sometimes play unfair making their products work for a specific Chinese mining pools. They don't care about other pools and provide no support.
6. ASIC manufacturers are not disclosing any information regarding their products not allowing people modify the hardware/firmware by

default. Who are they playing for? Crypto World? Decentralization? Miners? No. Only their own money matters.

7. The last but not least. Have you ever compared a GPU and a crypto ASIC device. A GPU usually is a cool welldesign nicelybuilt product. ASIC always looks like sh*t and works like sh*t. That simply means that ASIC manufacturers do not care. All they need to get is MONEY. And asap.

> **haione** | 1 point written 13 days ago ago
> full ack!

BackOnTheBike | 1 point written 14 days ago ago
ProgPow is a waste of time and energy.. our focus should be else where.

> **alsomahler** | 2 points written 14 days ago ago
> Don't worry, only the people who care will put their time and energy in this. People like you who care about more important things will just ignore this keep on building.

Darius510 | 2 points written 14 days ago ago
Man this is exhausting.

I'm a victim of mineority's complete failure, to the tune of several thousand dollars.

If I can look past the origin of the code, anyone can.

If the increasing desperation of your social media campaign is anything to go by, ProgPoW is going to work extremely well, and you know it.

haione | 2 points written 14 days ago ago
the reputation of asic manufacturers from eastern hemisphere gone down the road for reasons. linzhi doing pretty good job to make it even worse.

hitmybidbitch | 1 point written 14 days ago ago
You are complete garbage.

greerso | 1 point written 14 days ago ago
You are asking if a cure for cancer created by Mao Zedong is any less valuable than a cure created by Mother Theresa?

What you should be asking is does it work and what the side affects are.

Crypto_Economist42 | 1 point written 13 days ago ago
"written guarantee from Nvidia to not favor selected miners with secret optimizations or special chip deals" do you have any proof of this conspiracy theory?

The latest benchmarks show AMD has better hashrate/watt. FYI

jps_ | 0 points written 14 days ago ago
We should stay above the adhominem attacks here. Instead focus on facts, figures, and what we can prove. that's the foundation of the opensource movement.

So far, there are no facts that "asics are bad' as an apriori statement. Just bad if they represent a centralizing function... but if that's bad, then PoS sucks... so... not bad, apriori. There are also no facts that suggest ASICs are prevalent. In fact, everything triangulates to the fact that they are an irrelevant contributor to current hashpower, and subject to being overtaken by tweaking of commodity

GPUs (which are also ASICs). Finally, the stated intention of Ethereum is to move to PoS, in which all mining is irrelevant, and nobody's having the discussion to ditch PoS.

Thus, all this fuss about an ASIC resistant algorithm is about something that nobody can prove is bad, against something nobody can prove exists, for a purpose everyone agrees is ultimately irrelevant.

Basically, it's a shortterm, shortsighted tempest in a teapot. Probaby fomented by vested interests.

Which does leave just about everyone wondering and speculating about what it could be. The fact that the spokesperson has a less than spectacular past adds fuel to this fire. But I think if we stick to the real agenda which is that ASICs aren't bad as long as they are commodity oriented, that they aren't prevalent even if they are bad, and that even if they are prevalent, and even if they are bad, it's a speedbump in the roadmap.

Can we all just grow up and move past this?

> **greerso** | 2 points written 14 days ago ago
> ProgPoW is not an antiasic strategy, its a strategy to make sure that **all** hardware performs evenly. I dont mean that in a socialist way where a $50 gpu will perform the same as a $3000 asic, I mean that relatively they will perform evenly.
>
> In the case of Ethereum there is a strong argument against fixed function hardware in that a gpu is reusable so gpu miners will be more willing to encourage a move to PoS. A fixed function asic on the other hand will have no value beyond PoS, see BTC/BCH hash wars to understand what damage large centralized forces controlling most of the network hash can do and in that war their investments weren't even at risk of being bricked.
>
> > **jps_** | 1 point written 14 days ago ago
> > Yes, but this fails to answer "who cares"? except folks who have GPUs and don't want to be disadvantaged by some new hardware that they don't have.
> >
> > What you are saying is that miner rewards should be distributed "status quo" regardless of any new hardware on the horizon. But who says that should be a rule?
> >
> > Moore's law means that this will happen no matter what we do.
> >
> > As far as repurposing gpus means miners will be more willing to move to PoS... that's pretty much irrelevant: PoS will happen regardless of whether miners let it happen, it's not like they can stop it now.
> >
> > As far as this:
> >
> > > A fixed function asic on the other hand will have no value beyond PoS, see BTC/BCH hash wars to understand what damage large centralized forces controlling most of the network hash can do and in that war their investments weren't even at risk of being bricked.

This is cherry picking. We have our own ETH/ETC wars which happened without ASICs. Tribal is as tribal does. Mac versus PC, Google vs Apple, EthX vs EthY... Republicans vs Democrats... Humans have been tribal since before the dawn of civilization, and that's not going to stop. If you stop one form of tribalism you'll just see a different form stand up. It's pointless.

greerso | 2 points written 14 days ago ago

> What you are saying is that miner rewards should be distributed "status quo" regardless of any new hardware on the horizon. But who says that should be a rule?

I actually attempted to make the point contrary to this. New hardware with new tech such as GDDR6 or HBM3 will, and should, outperform older inferior hardware, this comes with a price tag. What will not happen is that GDDR5 will outperform GDDR5 or $500 hardware will not outperform $1000 hardware. It will not matter what kind of boards and enclosures you package this silicon in.

> This is cherry picking. We have our own ETH/ETC wars which happened without ASICs. Tribal is as tribal does. Mac versus PC, Google vs Apple, EthX vs EthY... Republicans vs Democrats... Humans have been tribal since before the dawn of civilization, and that's not going to stop. If you stop one form of tribalism you'll just see a different form stand up. It's pointless.

Again, not the point I was attempting to make. Protecting a multi million dollar investment is not tribalism.

jps_ | 1 point written 14 days ago ago

> Protecting a multimillion dollar investment is not tribalism.

It's actually the whole point of a tribe: protecting what is inside whatever binds the tribe together, against the forces outside the tribe. You may not see it as such, but there is very clearly a "GPU" tribe doing its best to diss the ASIC tribe, and vice versa. It may not be evident from inside one of the tribes, but it sure as heck is evident from the sidelines.

As far as my point about inevitability of hardware obsolescence:

> I actually attempted to make the point contrary to this.

And then you go on to describe which parts of hardware obsolescence you have no objection against, while mounting an argument that is entirely against hardware (GPU) obsolescence.

> New hardware with new tech such as GDDR6 or HBM3 will, and should, outperform older inferior hardware, this comes with a price tag. What will not happen is that GDDR5 will outperform GDDR5 or $500 hardware will not outperform $1000 hardware. It will not matter what kind of boards and enclosures you package this silicon in.

It's selective at best and specious logic. Why are you OK with $1000 hardware outperforming $500 hardware without being OK that maybe the $500 difference in hardware cost could in fact be an ASIC??

Your argument is not standing on firm principles here, because you are being selective in your position.

Special purpose technology is often beneficial, although it almost always hurts the incumbent ecosystem. Automobiles are very custom engines, with the sole purpose of taking people from point A to point B. Back in the days of horses, we also had engines, and we also had the entire carriage industry up in arms against these horseless carriages, because their investment in horses and barns was about to be made obsolete. The result of active lobbying by horse cart industry includes laws to have people walk in front of cars. This had the intended consequence of making cars more expensive and less practical, versus the espoused consequence of being safer. But it's patently ludicrous, in hindsight.

I'm not just picking one example. Personal computers were attacked by the mainframe industry. ATMs really messed up the lives and occupations of millions of tellers. The Internet destroyed "long distance minutes" as a business. There are millions of miles of perfectly good copper wire in the ground to every house in the US... rotting.... because we have wireless phones instead...

Innovation happens and special purpose devices whether ASIC or not intervene and render trillions of dollars of capital obsolete. GPUs occupy no special pedestal in technical Darwinism, and it is absurd to treat them as some sacrosanct technology. Regardless of how loud the priests of the GPU tribe are shouting.

Cryptocurrency itself is disrupting banks, and it's deliciously ironic that a faction within a disruptive technology movement is up in arms against an internal disruption of its own technology!

If there's a device that mines just as much ETH for a fraction of the electricity, anyone who cares about the planet will want it to succeed. Even if it means the starvation of the GPU tribe. So has it ever been, so will it always be.

greerso | 2 points written 14 days ago ago

> It's actually the whole point of a tribe: protecting what is inside whatever binds the tribe together, against the forces outside the tribe. You may not see it as such, but there is very clearly a "GPU" tribe doing its best to diss the ASIC tribe, and vice versa. It may not be evident from inside one of the tribes, but it sure as heck is evident from the sidelines.

Symantecs. My point is about who is incentivized to protect the network.

You have incorrectly assumed that my stance is anti asic. I do not care what the hardware is, I care about making the hash as decentralized as it can be or crypto assets have no value to me. I would like to see other PoW algorithms adopt ProgPoW and I would like to see those networks mined by various hardware types, GPU's if hobbyists continue to want to do that, ASIC's for plug and play convenience, hybrid gpu/fpga's, even GPU's in a plug and play enclosure with ready to mine software.

> If there's a device that mines just as much ETH for a fraction of the electricity, anyone who cares about the planet will want it to succeed. Even if it means the starvation of the GPU tribe. So has it ever been, so will it always be.

You talk smart, surely you understand that the W in Proof of Work is measured by the energy spent on it. If you're spending less energy, you're working less. Each time energy is saved, more devices are added, difficulty goes up and no extra security or energy savings was accomplished.

Before you go on and paint me as Tribe GPU again. I'll say this one last time. I am an owner and supporter of GPU's, ASIC's and FPGA's. I will support and purchase whatever else comes next.

jps_ | 1 point written 14 days ago ago

> You have incorrectly assumed that my stance is antiasic.

But you are proProgPOW. The only purpose of ProgPOW is to be antiasic. It has no other value. I assumed your stance proProgPOW was aligned with its only purpose. Apologies if i got that wrong, but if you aren't proGPU then what the heck is the point of being proprogPOW? Make work?

> I would like to see other PoW algorithms adopt ProgPoW

Why? It's just an algorithm. How about if they use ETHHash? Personally, I would prefer if ETHHash becomes as prevalent as 802.11, which only occurred when there were chips for that. Why not have chips for ETHHash and drive it into everything? Why should everything come with a GPU and only a GPU and never evolve past that? Unless of course one is a member of tribeGPU, in which case totally understandable.

I want the same thing. I am arguing from the basis of history which suggests that the fastest path to ubiquity is to embed functionality in cheap silicon, and not entrench it in expensive $500a pop GPUs.

Proprietary advantage is not how the endgame emerges. Otherwise, Texas Instruments would own the entire PC market. And they don't.

> I care about making the hash as decentralized as it can be or crypto assets have no value to me.

Me too. But let's take that apart.

First, I detect ZERO evidence that ASICs are a cause of centralization. In fact, although they are widely assumed to exist, all evidence requires that they are remarkably broadly distributed, and therefore just as benignly centralizing as GPUs. Mining farms are *far* more of a centralizing force than "ASICs", and we don't seem to have anyone railing against these.

Second, "*making the hash as decentralized as it can be*" that doesn't have to be antiASIC on an apriori basis. Bitcoin seems to be surviving (in fact dominating) and it's algorithm is completely dominated by ASIC. So you are arguing a non sequitor in the face of the only evidence that exists. Diverting ETH Devs to implement ProgPOW is taking away resources from usable applications,

from PoS, and from all kinds of things. It's a side show to the main event.

> surely you understand that the W in Proof of Work is measured by the energy spent on it.

No, I do not understand this, because it is wrong. The "W" in proof of work is measured in hashes per unit time. That happens to correlate to the energy spent, but is only 1:1 between devices that have the same energy cost per hashesper second. A device that generates the same number of hashespersecond at 1/10 the energy generates the same WORK (the W), but 1/10 the energy cost. It isn't accidental that we don't call it PoE.

Sorry, but I am not so easily fooled.

> Each time energy is saved, more devices are added, difficulty goes up and no extra security or energy savings was accomplished.

Again, not true.

Mining is a tournament business: adding more miners does not increase the number of ETH that are mined, because difficulty algorithm adjusts. It does change who gets the ETH that is mined. When we are at equilibrium, and there is a distribution of energycost per unit hashper second, what it means is that less efficient (and costly) devices become less profitable and drop out, and more energy efficient devices take their place, and the hashpower remains constant, if the devices coming in cost the same as the devices going out.

If there is a cost advantage to the energy efficient devices, and energy is the *only* cost, then yes, the total hashpower would go up by a factor of 10 and then the ETH reward per unit energy would not change. But since there is a capital cost of hardware that needs to also be considered, and this is nontrivial compared to the energy cost, and needs to be compensated by the ETH that is earned, the net energy cost of the same amount of hashpower is lower.

> Before you go on and paint me as Tribe GPU again.

Apologies. I wasn't talking about you perse, but as a voice of the proprogPOW constituency, which is dominated whether knowingly or unknowningly by the priests of the GPU tribe. I can't tell whether you are a priest in disguise, or one of the brainwashed flock, or just someone advancing an argument that doesn't rest on the reasons they think it does. But "you" is meant collectively.

if it looks like a duck and quacks like a duck, not my fault if I lump it in with all the other ducks.

> **greerso** | 1 point written 14 days ago ago
>
> The only argument to say that ProgPoW is antiasic is that in order for an asic to be financially viable it must be able to monopolize the network hash. If this is true, then yes, I'm antiasic. I do not believe this to be true (even if it is slightly true today).
>
> ProgPoW is not a complete PoW algorithm, its a design philosophy that can be applied to any memory hard PoW algorithm. Instead of leaving space for an inefficient arms race, it it forces the hardware to work hard.
>
> One algo for all chains is dangerous for all but the dominant chain. See every single 51% attack.
>
> A measurement in hashes is meaningless, the energy consumed to solve a hash is what matters. Go back to the principles behind Proof of Work, even before Blockchain. Work comes at a cost, that is why we value it. If few parties can hash the same while expending less energy their signals (hashes) are not as trustworthy because they are not expending as much energy to perform the work as the rest of the network. If all of the network can hash more for less energy, they will keep buying devices. Hardware is an asset, energy spent is a liability. Hardware costs are recouped in a relatively short period of time. See https://medium.com/@OhGodAGirl/theproblemwithproofofworkda9f0512dad9
>
> With regards to the short period of PoW left on ethereum, I am antiasic and maybe this is where I look and sound like a duck. The change from PoW to PoS is my reason for this. New eth asic's are coming, it is in the
>
> interest of the companies making those asics

and the purchases of them to make a fork to PoS a contentious one, whether or not they are successful will not matter for all the bad press it will cause further sullying the name of crypto.

jps_ | 1 point written 13 days ago ago

> The only argument to say that ProgPoW is antiasic is that in order for an asic to be financially viable it must be able to monopolize the network hash.

Wrong. In order for an ASIC to be viable it has to give miners a marginally better return on investment than mining with a GPU. Period. The same can be said about the next generation of GPU. If either ultimately displace less capitalefficient mining rigs, previous generations of GPUs, whatever, that's a consequence of economic Darwninism, not an apriori requirement for an "ASIC", or a "GPU".

Also, ProgPOW is "anti ASIC" merely and precisely because it is pro "only GPU". This is by design and no amount of fancy language footwork changes this fact. If you are a member of the "Only GPU" tribe, then you clearly not a member of the "somethingthatisn'ta GPU" tribe. Whether you admit it or not.

> Instead of leaving space for an inefficient arms race, it it forces the hardware to work hard.

Come on, now you are just coloring inside the lines. ProgPOW forces **GPU** hardware to work hard, and it forces anything that isn't a GPU to be exactly like a GPU if it wants to work at all. Which is to say, it forces only GPUs.

> The change from PoW to PoS is my reason for this. New eth asic's are coming, it is in the interest of the companies making those asics and the

> purchases of them to make a fork to PoS a contentious one, whether or not they are successful will not matter for all the bad press it will cause further sullying the name of crypto.

Oh dear, it appears you haven't been paying attention.

First, a "fork" to PoS isn't happening. There is no fork, which is the elegant finesse of Shasper. Once Constantinople goes through, everything necessary to shift to PoS can happen *WITH NO FORK*. this is why it was so important to delay Constantinople until the miners are up against a wall.

Second, even without ProgPOW, when ETH shifts to PoS, what precisely do you think 150 Terahash worth of GPUs are going to do? Roll over and play dead? We saw what 10 TH of GPUs heading over to ETH Classic did. There already isn't enough altcoin hashing to absorb all the GPUs on Ethereum, let alone ASICs. That problem is already yours to navigate. Multiplying the participants by two isn't going to make it twice as bad. Ultimately, you are suggesting to defend against the oncoming tsunami by building a sandcastle. Not very wise.