Linzhi Semiconductors

Linzhi Working Papers
No 14

On Whistleblowing.

by Sonia Chen

September 2019

Keywords: LWP14, Ethereum, Whistleblowing, Predator, Anonymity

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

On Whistleblowing

Linzhi ASICs
Sep 21 · 8 min read

We know more than what we have talked about so far.
We know but we cannot prove.

There are two types of knowledge: A priori and a posteriori knowledge.

A priori and a posteriori
The Latin phrases a priori ("from the earlier") and a posteriori ("from the later") are philosophical terms...
en.wikipedia.org

Our knowledge about the attack on Ethereum is a posteriori knowledge, so we don't need to ask anyone, and we don't need proof ourselves.
We know.
A posteriori are empirical facts unknowable by reason alone.

Since we don't want to ally with the attackers, and we have no proof that would satisfy an audience that is tired in a world of fake

news and FUD, what we decided to do is to try to open up eyes about what might be going on — plausibilities, motivations, personal and corporate backgrounds.
We do this for 9 months now, it binds a significant amount of our resources.
That is all we can do.

. . .

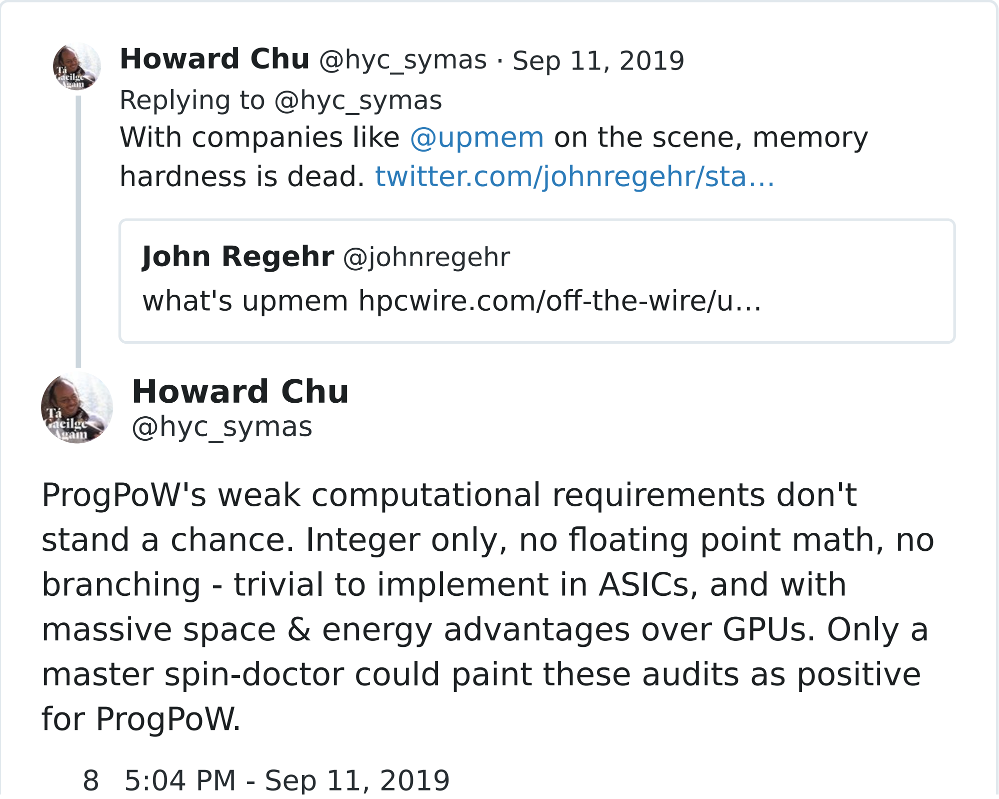
Bob Rao's Audit

We are disappointed that so few independent Ethereum developers seem to read and think about Bob Rao's excellent audit.

https://github.com/ethereum-cat-herders/progpow-audit/raw/master/Bob%20Rao%20-%20ProgPOW%20Hardware%20Audit%20Report%20Final.pdf

From our view, Bob Rao's audit confirms that ProgPoW will not achieve its goal of closing the efficiency gap between ASICs and GPUs, which adds to a list of people that have come to the same conclusion.

1. Howard Chu



Howard Chu @hyc_symas · Sep 11, 2019
Replying to @hyc_symas
With companies like @upmem on the scene, memory hardness is dead. twitter.com/johnregehr/sta...

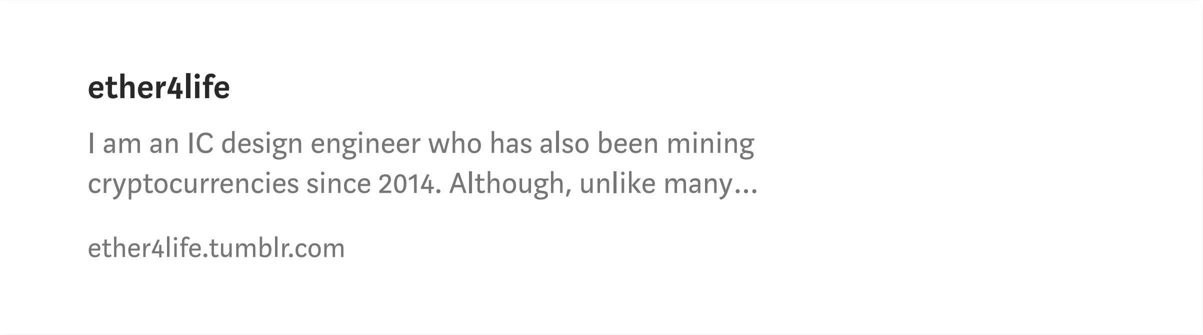
John Regehr @johnregehr
what's upmem hpcwire.com/off-the-wire/u...

Howard Chu
@hyc_symas

ProgPoW's weak computational requirements don't stand a chance. Integer only, no floating point math, no branching - trivial to implement in ASICs, and with massive space & energy advantages over GPUs. Only a master spin-doctor could paint these audits as positive for ProgPoW.

8 5:04 PM - Sep 11, 2019

2. ether4life



ether4life

I am an IC design engineer who has also been mining cryptocurrencies since 2014. Although, unlike many...

ether4life.tumblr.com

> “This results in a 4x advantage in terms of energy efficiency over a GPU for ProgPoW” — ether4life

(An anonymous Ethereum freedom fighter. We tried to track down who this person is, unsuccessfully. Please come forward privately if you read this.)

3. Tim Olson

https://ethereum-magicians.org/t/progpow-audit-delay-issue/3309/47

> “they are using more chip, which means more up-front cost (capex), but there will be a lot more power too (opex)” — Tim Olson

4. Linzhi

EIP 1057 (ProgPoW): Open Chip Design for only 1% cost/power increase EIP 1057 (ProgPoW)…

How to add ProgPoW to your ASIC.

medium.com

Against all this, EIP 1057 states right in its abstract https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1057.md

> *ProgPoW is … designed to close the efficiency gap available to*

> *specialized ASICs.*

It has now been sufficiently established that EIP 1057 fails to reach its main stated design goal.

That *alone* is enough to reject EIP 1057 on technical grounds. Why should Ethereum adopt a technology that doesn't do what it says it will do?
It is enough to reject EIP 1057 without further input or agreement from its authors.

One must assume the EIP 1057 authors to respond to arguments with new arguments, but as engineers we should be able to think independently through the facts and come to our own judgment, and reject what we understand to be false.

We don't need to speculate about business motives, mining fairness and other PoW algo change related risks.

. . .

Linzhi and Hudson Jameson

We surely made many mistakes in our whistleblowing journey. We may have construed connections with our bias. We followed dead-end leads. We used over-emotional language.

There was also a positive side: New friends, finally understood the

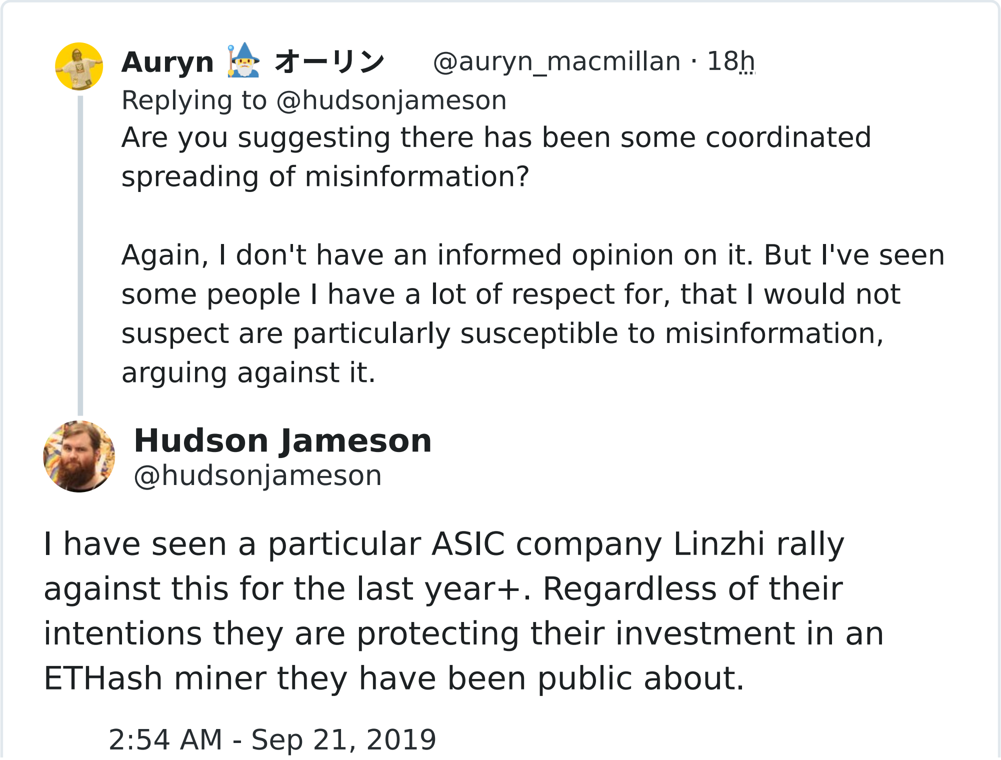
power of FUD and that FUD must be rejected the same way we reject hate speech.
Learned a lot about bias
https://en.wikipedia.org/wiki/List_of_cognitive_biases

We can say nothing but positive things about Hudson. Hudson is the greatest guy that could chair the all core devs. Hudson leads with integrity in an environment of horrendous intensity, like an ongoing F1 race.
If Hudson thinks Linzhi is not to be trusted, we can accept that. We will try to earn his respect the same way we try to earn respect from anyone.

We communicate with Hudson for 9 months now. None of us has ever met him. Our communication was 90% public, 99% one-directional (from us to him), plus some attempts to start an email conversation, basically repeating the same things we said publicly and maybe a few more speculative (to him) thoughts. I believe Hudson never replied.

He was and is faced with a very difficult situation: A team of malicious actors is attacking Ethereum, and the format of publicly recorded all-core-dev calls with a 100% engineer ratio is the perfect entry point for the attackers.
He wants to be neutral because Ethereum wants to be a neutral platform, but a team of collaborators cannot be neutral when faced with a predator, see Rick Falkvinge’s thoughts on that in the next section.

To maintain our own integrity, I will reply to Hudson's tweets about Linzhi here, rather than taking it to Twitter.



Auryn 🧙 オーリン @auryn_macmillan · 18h
Replying to @hudsonjameson
Are you suggesting there has been some coordinated spreading of misinformation?

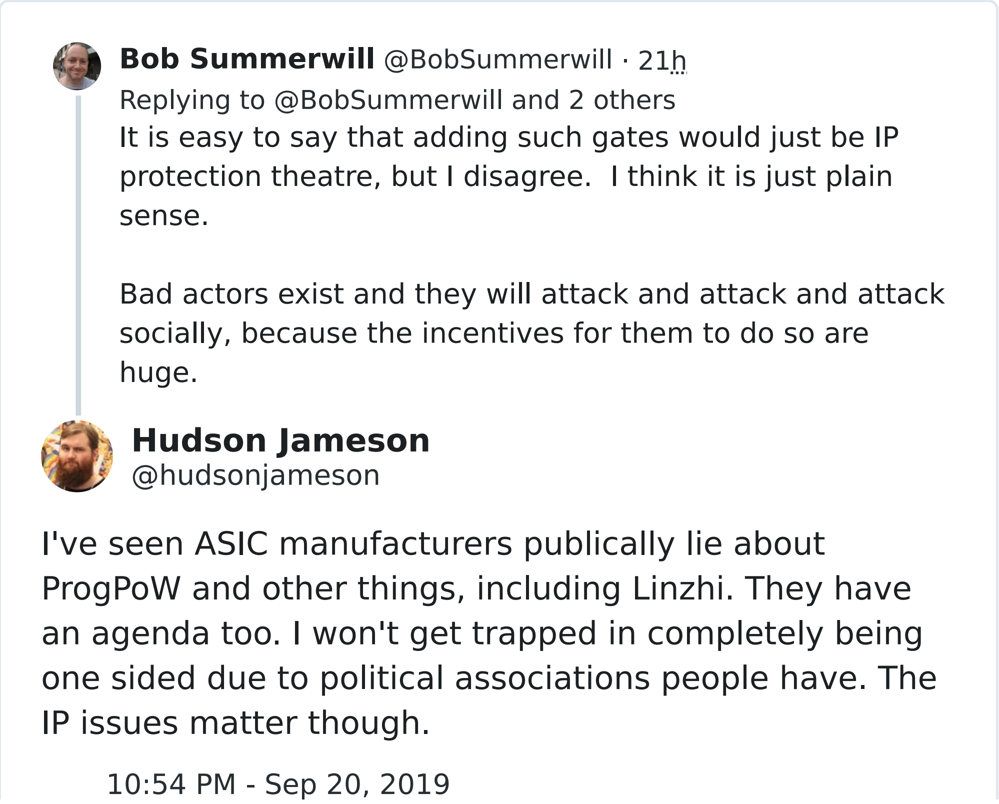
Again, I don't have an informed opinion on it. But I've seen some people I have a lot of respect for, that I would not suspect are particularly susceptible to misinformation, arguing against it.

Hudson Jameson
@hudsonjameson

I have seen a particular ASIC company Linzhi rally against this for the last year+. Regardless of their intentions they are protecting their investment in an ETHash miner they have been public about.

2:54 AM - Sep 21, 2019

> *A: We are protecting our investment into an Ethash miner via the fight for the viability of the entire platform. The two motivations are inseparable for us.*



Bob Summerwill @BobSummerwill · 21h
Replying to @BobSummerwill and 2 others
It is easy to say that adding such gates would just be IP protection theatre, but I disagree. I think it is just plain sense.

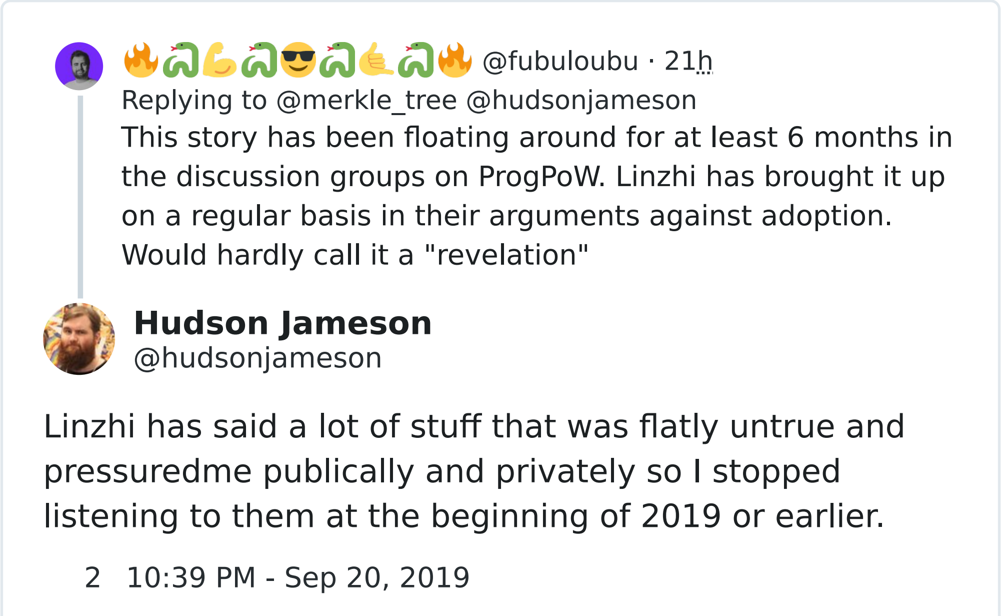
Bad actors exist and they will attack and attack and attack socially, because the incentives for them to do so are huge.

Hudson Jameson
@hudsonjameson

I've seen ASIC manufacturers publically lie about ProgPoW and other things, including Linzhi. They have an agenda too. I won't get trapped in completely being one sided due to political associations people have. The IP issues matter though.

10:54 PM - Sep 20, 2019

> *A: At some point neutrality and decision-making are mutually exclusive. If you are neutral forever you are setting up the perfect environment where a hidden agenda will succeed. Doacracy cannot work, in a doacracy the bank robber will just claim to be the CEO of the bank and get away with the robbery. Please point out what you believe our lies were so that we can reconsider the messaging or correct mistakes. We maintain a list of all substantive contributions to the debate at https://linzhi.io*



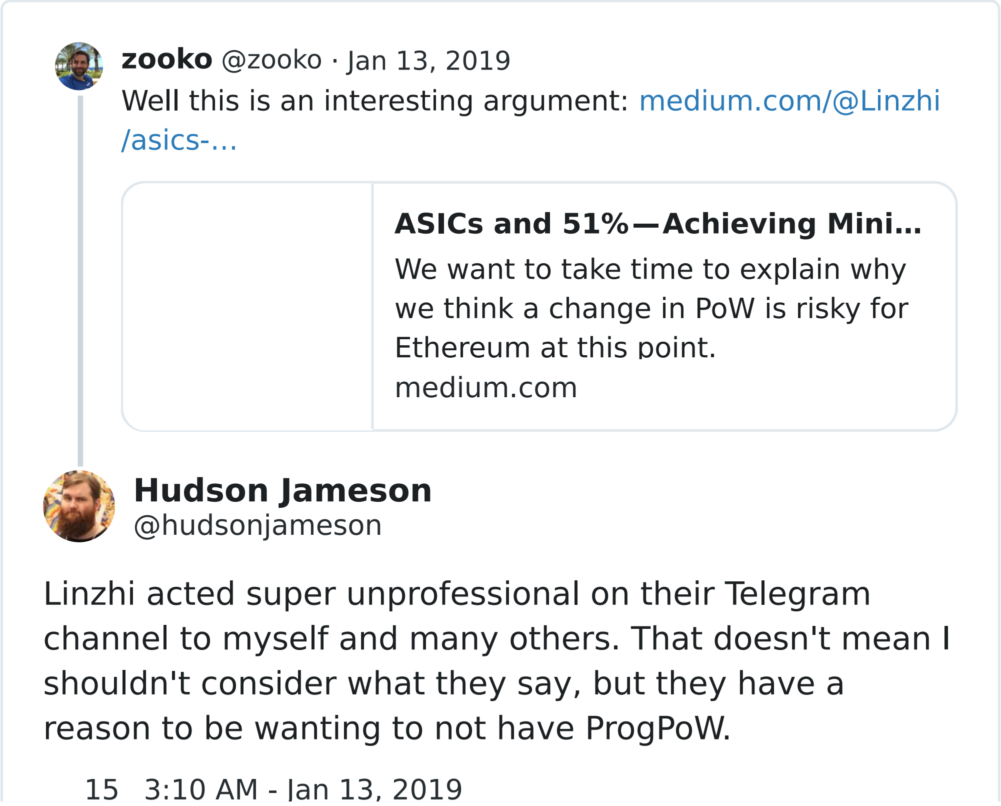
🔥🐍💪🐍😎🐍🤙🐍🔥 @fubuloubu · 21h
Replying to @merkle_tree @hudsonjameson
This story has been floating around for at least 6 months in the discussion groups on ProgPoW. Linzhi has brought it up on a regular basis in their arguments against adoption. Would hardly call it a "revelation"

Hudson Jameson
@hudsonjameson

Linzhi has said a lot of stuff that was flatly untrue and pressuredme publically and privately so I stopped listening to them at the beginning of 2019 or earlier.

2 10:39 PM - Sep 20, 2019

> *A: There was no other known person that offered themselves as a recipient of whistleblowing-like information. We tried to contact people at the Ethereum Foundation, I believe noone ever replied. Big credits go to you for coming to our Telegram after seeing the Coindesk article. If you feel we pressured you unduly, I apologize. Same as before, please find the time to point out what you believe was flatly untrue so we can reconsider and correct. Thanks!*



zooko @zooko · Jan 13, 2019
Well this is an interesting argument: medium.com/@Linzhi/asics-...

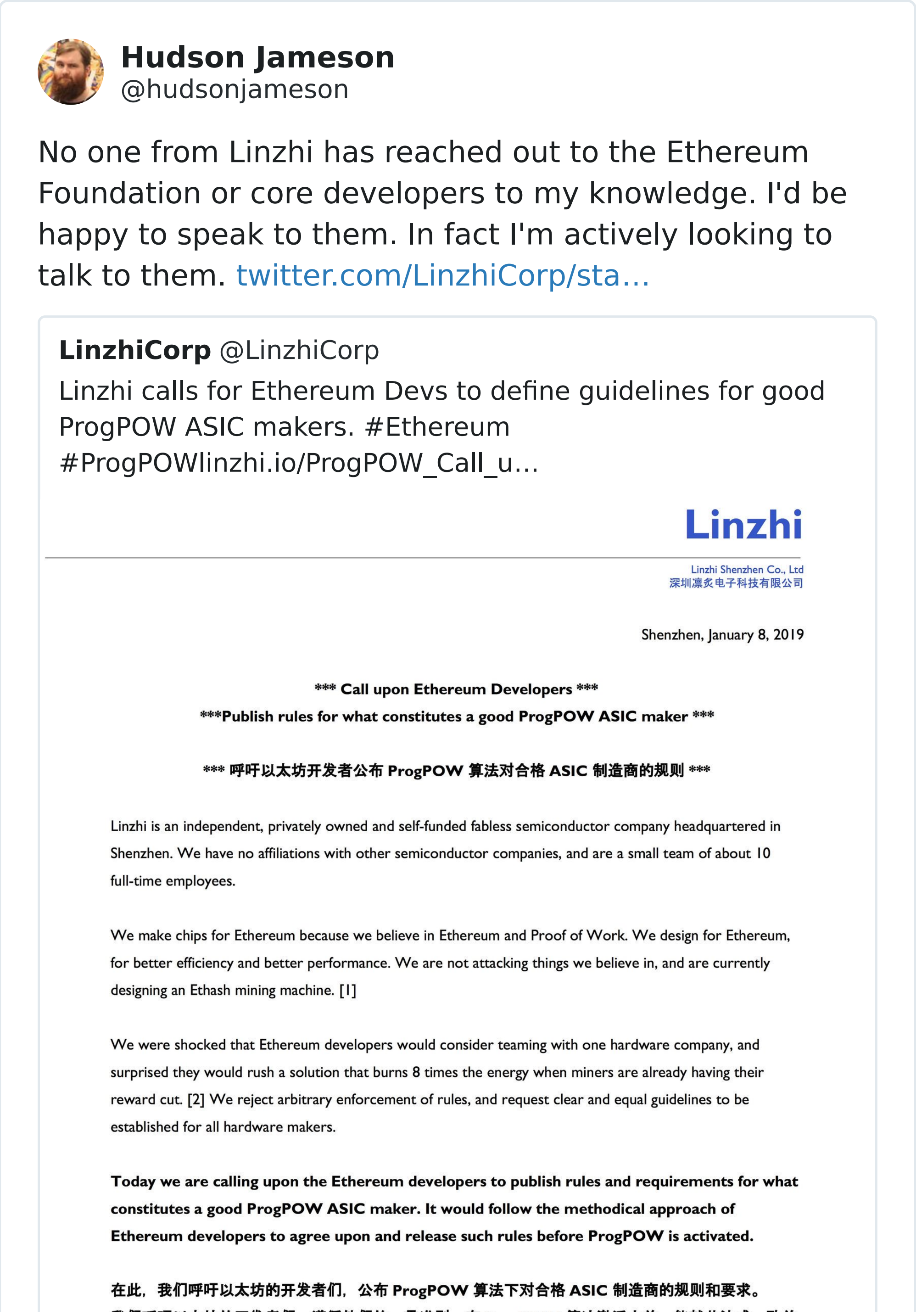
ASICs and 51%—Achieving Mini...
We want to take time to explain why we think a change in PoW is risky for Ethereum at this point.
medium.com

Hudson Jameson
@hudsonjameson

Linzhi acted super unprofessional on their Telegram channel to myself and many others. That doesn't mean I shouldn't consider what they say, but they have a reason to be wanting to not have ProgPoW.

15 3:10 AM - Jan 13, 2019

> *A: Our Telegram chat from this time is archived, with permission from Hudson, in "LWP5 Linzhi Telegram January 7 to 29, 2019. Lessons Learned."*
> *We were emotional, and the attackers were in our Telegram in full force. Today we have banned any and all accounts we believe to be associated with the attackers, and it's much nicer again.*
> *You are still in the group Hudson, if you have ASIC related questions — just ask.*



Hudson Jameson
@hudsonjameson

No one from Linzhi has reached out to the Ethereum Foundation or core developers to my knowledge. I'd be happy to speak to them. In fact I'm actively looking to talk to them. twitter.com/LinzhiCorp/sta…

LinzhiCorp @LinzhiCorp
Linzhi calls for Ethereum Devs to define guidelines for good ProgPOW ASIC makers. #Ethereum #ProgPOWlinzhi.io/ProgPOW_Call_u…

Linzhi

Linzhi Shenzhen Co., Ltd
深圳凛炙电子科技有限公司

Shenzhen, January 8, 2019

***** Call upon Ethereum Developers *****
*****Publish rules for what constitutes a good ProgPOW ASIC maker *****

***** 呼吁以太坊开发者公布 ProgPOW 算法对合格 ASIC 制造商的规则 *****

Linzhi is an independent, privately owned and self-funded fabless semiconductor company headquartered in Shenzhen. We have no affiliations with other semiconductor companies, and are a small team of about 10 full-time employees.

We make chips for Ethereum because we believe in Ethereum and Proof of Work. We design for Ethereum, for better efficiency and better performance. We are not attacking things we believe in, and are currently designing an Ethash mining machine. [1]

We were shocked that Ethereum developers would consider teaming with one hardware company, and surprised they would rush a solution that burns 8 times the energy when miners are already having their reward cut. [2] We reject arbitrary enforcement of rules, and request clear and equal guidelines to be established for all hardware makers.

Today we are calling upon the Ethereum developers to publish rules and requirements for what constitutes a good ProgPOW ASIC maker. It would follow the methodical approach of Ethereum developers to agree upon and release such rules before ProgPOW is activated.

在此，我们呼吁以太坊的开发者们，公布 ProgPOW 算法下对合格 ASIC 制造商的规则和要求。

> *A: That is true. Before the core developer meeting January 4th we had not been in contact with core developers. Exactly as the Coindesk article says, we were shocked by the move of only working with one hardware company. That’s when we started to reach out.*

Ethereum Miner Linzhi Calls Out Project Coders for Proposed ASIC Ban - CoinDesk

Shenzhen-based miner manufacturer Linzhi has published a statement in response to a "tentative"...

www.coindesk.com

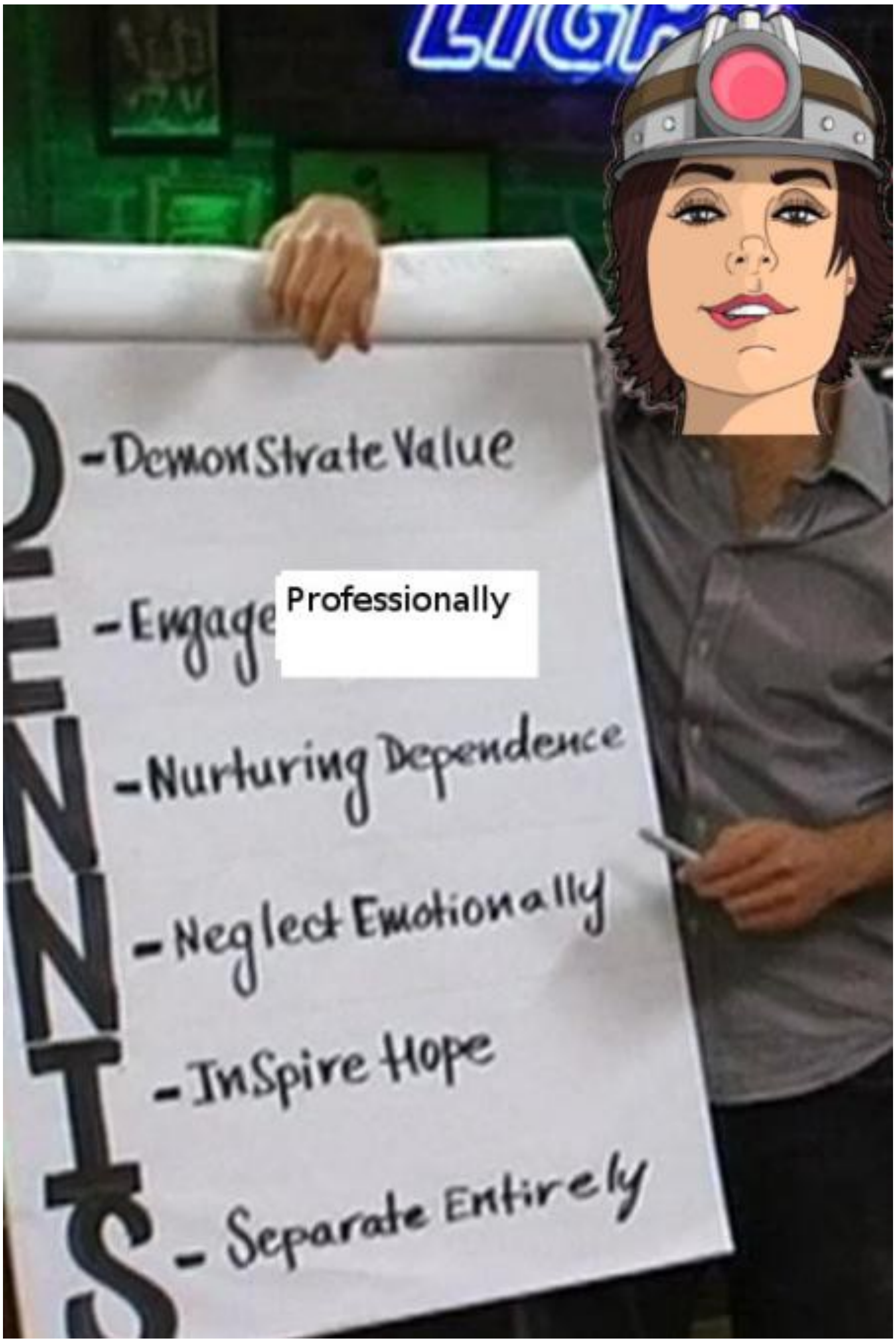
Thanks Hudson for everything you do for Ethereum! You *are* trying hard to maintain neutrality and we would be the last ones to criticize you for that.

. . .

Predators and Collaborators

The ProgPoW team among Ethereum developers, is a predator among collaborators.

> *These predators hide among collaborators. They try to exhibit signs that make the collaborators see the predators as a collaborator, and then, when the time is right, they prey. It is not possible to imagine what these people are capable of. You cannot warn people who have not experienced a predator about what is likely to happen. Their behavior is simply inconceivable among people who are conditioned to collaborate. They do not feel embarrassment at lies. This is one defining factor. They are incapable of feeling embarrassment in the face of making outrageous lies.*
> *When they are giving out outrageous lies, what they are feeling is something akin to a fisherman trying a new bait on their hook. No more.*
> *People who see the signs can't warn others, because they will be met by disbelief.*



A collage floating around the Internet by people trying to warn others about the official ProgPoW author.

. . .

Chipmakers and Collusion

In the context of PoW, it is important that a chipmaker treats all customers equally. To us crypto engineers this is obvious, but to chipmakers that is a new thing. A chipmaker may initially not understand the intricacies of “global hashrate and difficulty”, and what that means in terms of cutting deals with large clients that come forward to propose a deal.

If a chipmaker shares optimizations, specialized or unsellable chips, offers delayed payments or revenue sharing to individual mining clients, they are colluding against their other customers.

Analyst says Nvidia lied about its cryptocurrency earnings to avoid stock crash

Nvidia has been hit hard by the cryptocurrency crash, possibly worse than any other company. In November…

www.techspot.com

The best answer to this problem in our opinion is to demand transparency and to foster competition. Currently there are 4 viable chipmakers competing in the Ethash mining market: Nvidia, AMD, Bitmain, Innosilicon.
With the collusion risk clearly understood, one must avoid any action that rewards monopolization efforts by a chipmaker, and instead try to motivate new entrants such as Linzhi to enter the market.
We think it’s good news that in addition to Linzhi there are multiple other teams trying to design competitive Ethash chips or FPGA solutions.

We wrote about the risks of the collaboration between Nvidia and Core Scientific in January, and encourage interested readers to revisit that.

ASICs and 51% — Achieving Mining Dominance How cost advantage drives centralisation.

We want to take time to explain why we think a change in PoW is risky for Ethereum at this point.

medium.com

. . .

Dark Empire and Fix

Anonymous and decentralized value networks attract many people.
If you would be running a successful business line around stock fraud and money laundering, for example, you would see the chance to substantially reduce your operational risks.
Crypto mining (PoW and PoS) means cash-in, crypto-out. Cash losses become trading profits. You would want a media organization to orchestrate price swings you know about in advance.

Bob Summerwill started an important debate around anonymity of users versus anonymity of developers, and certificates of origin.

Developer Certificate of Origin

Developer Certificate of Origin Version 1.1 Copyright (C) 2004, 2006 The Linux Foundation and its contributors. 1…

developercertificate.org

The anonymity of users in our value networks is what we want to uphold, but we must be realistic and cold-blooded, maybe even cynical, about who some of those anonymous users will be and how we can avoid that they infiltrate the culture and community of the builders of the network.

Because if they do, it’s all over.

. . .

Linzhi Team, Shenzhen, 2019-Sep-21
Telegram: t.me/LinzhiCorp

About Linzhi: If you have questions about ASICs, please feel free to come to our Telegram group LinzhiCorp and ask whatever is on your mind.
If you are a known community member or developer with good reputation, casually feel invited to come to our office and factory in Shenzhen.

Linzhi believes that bridging the hardware-software gap is critical for crypto to succeed.
We don’t want crypto to be confined to a world of papers and

github commits. PoW was a key innovation to connect the world of software with the world of energy and time. Hardware wallets, gas turbos, accelerators for signing, proving, verifying, sorting and other things are on the horizon.

We will continue to contribute to the Ethereum platform as a chipmaker.