

 SEARCH


 What are you looking for?

















 ROOMS & PEOPLE

No room search results...

CHAT MESSAGES

No message search results...



-  Danno Ferrin @shemnon Mar 21 13:28  
I will be honest. The tone of your comments make me less sympathetic to the pro-asic arguments. Independent of the technical arguments. Your instance on personal attack and mockery makes me think you are unsure of your own position and that the facts won't back you up. A more confident and respectful tone would have made a world of difference.
-  Sonia-Chen @Sonia-Chen Mar 21 13:36  
well thanks for reaching out and trying to raise the bar! I like Michelle Obama: when they go low, we go high! right?  
so I appreciate your comment  
I am close to leaving the public ETH gitters entirely, because they are overrun with fake accounts and people with massive second agendas  
I think we have made our points  
but I saw some things there from Peter and Greerso that are just so unbelievable... so yeah. the situation is extremely difficult for people who have no visibility into the mining business. it's a multi-billion USD industry
-  Danno Ferrin @shemnon Mar 21 13:37  
If you had started with a respectful tone I feel that there is a strong change ProgPow would not have happened. I've found the eth community tends to discount any argument attached to ad-hominim attacks.
-  Sonia-Chen @Sonia-Chen Mar 21 13:38  
you realize we have these discussions for months, yes?  
the ETH community will find the best way forward. we are just a chipmaker.
-  Danno Ferrin @shemnon Mar 21 13:38  
yes. And your shift to personal attacks correlated with the rise in acceptance for ProgPow.
-  Sonia-Chen @Sonia-Chen Mar 21 13:39  
I would hope it's not that easy to manipulate you guys  
if it is, no wonder progpow can do their play. noone asks tough questions and insists on an answer  
Kristy is a known scammer
-  Danno Ferrin @shemnon Mar 21 13:40  
Look at how the community reacted to the afri situation. Many have an allergic reaction to personal attacks, regardless of who it is to.
-  Sonia-Chen @Sonia-Chen Mar 21 13:40  
it's just a fact  
who bullied afri out?
-  Danno Ferrin @shemnon Mar 21 13:40  
It is that he was bullied out, not who, that the community reacts to.
-  Sonia-Chen @Sonia-Chen Mar 21 13:40  
you don't see the connections we are seeing, because we see the business, the money flow  
not the code  
of course, good!  
if you have questions, I am happy to answer  
if not, also ok  
I think the risk of a contentious fork is LESS than most people think
-  Danno Ferrin @shemnon Mar 21 13:41  
I think a lot of the eth community would rather lose than win by the politics of personal desctruction. That is their nature.
-  Sonia-Chen @Sonia-Chen Mar 21 13:42  
I use this chance of a confidential chat. to the best of our understanding, it was in fact Vitalik who kicked off the progpow project with Nvidia  
vitalik should be honest with the core devs and community members  
BUT  
he didn't realize that nvidia would sell out to large farms  
and give big discounts to Genesis, Core Scientific, maybe others  
ETH was always driven by engineering excellency  
not by corporate power battles and marketing stories  
progpow is a new chapter for ETH  
nvidia setup the core progpow team, it's about 15 people  
that's not the bad part. the bad part is that they sold out to large farms, including core scientific whose only customer is nchain (Craig Wright/Calvin Ayre)  
Hudson calls this "conspiracy theories"  
well then...  
oh, one last info for you:  
maybe there is a good chance you already don't believe me. "the bad ASIC makers" "evil this, greedy that"  
already last year Kristy came to us saying she wants to buy ASICs from us  
when we said we could do a progpow ASIC (we can, but probably won't), some weird guy showed up at our office in Shenzhen (the address is not generally published) and offered up to 75 mio USD for progpow ASICs!
-  Sonia-Chen @Sonia-Chen Mar 21 13:47  
crazy  
we kicked him out, he never entered our office  
the devs just don't understand what kind of business forces are at play behind the scenes. they have no visibility. Hudson has 1 E3 under his desk... :)
-  Danno Ferrin @shemnon Mar 21 13:49  
and he is open about his ownership and use of that E3. Public knowledge.
-  Sonia-Chen @Sonia-Chen Mar 21 13:49  
I know, that's my point  
ONE E3  
do you know how much capital is invested in the ETH security network?  
140 TH = 500k GPU rigs, plus 100k E3, plus datacenters: total invested capital around 1 billion USD  
1,000 millions  
monthly fees: 50 mio USD  
the devs lost control of this
-  Danno Ferrin @shemnon Mar 21 13:51

PEOPLE

 Linshi



So I am not opposed to ASICs. The issue is that Eth has a social contract from it's founding to be ASIC resistant and move to PoS. The PoS transition is taking longer than anticipated, so an algo shift keeps that social contract in place. It is that social contract that attracts many developers and give Eth it's community lead.



Sonia-Chen @Sonia-Chen Mar 21 13:51

yes, agreed

and I think so far the progpow discussions are still healthy

and ETH has the right to switch to progpow, and I think the switch can be successful!

the dangers I am seeing:

1. afri bullied out



Danno Ferrin @shemnon Mar 21 13:52

And ASICs are the future of crypto when it comes to permissionless store of value. But there is only room for one crypto to be secure per ASIC type.



Sonia-Chen @Sonia-Chen Mar 21 13:52

1. others being attacked now (alexey)



Danno Ferrin @shemnon Mar 21 13:52

Alexy is on point that state size is the biggest threat to Eth. Bigger than price and mining.



Sonia-Chen @Sonia-Chen Mar 21 13:53

yes!

you are right

ok let me back up a bit:

when progpow was started, it could have been rejected decisively at the beginning

but it wasn't

there is more than just code

if progpow is adopted, what are the consequences?

does that mean a future fork is more or less likely?

does that mean the transition to PoS will be easier or harder?

those questions are very hard to answer

for anyone!



Danno Ferrin @shemnon Mar 21 13:54

I think the PoS transition will be easier if PP passes. If PP fails it will be harder.



Sonia-Chen @Sonia-Chen Mar 21 13:54

ok!

I think it's the opposite, let me explain why:



Danno Ferrin @shemnon Mar 21 13:55

PP shows that the devs are comfortable "moving the cheese"



Sonia-Chen @Sonia-Chen Mar 21 13:55

an ASIC owner is tied to the network the ASIC secures

a GPU owner is not

the GPU owner can be much more aggressive

it is our genuine concern, ok? we are not making up stories to sell chips

we can be wrong!

yes, sure



Danno Ferrin @shemnon Mar 21 13:56

Yes, it increases the risk of 51% attacks. But then when Eth moves to PoS the GPU owners can move on.



Sonia-Chen @Sonia-Chen Mar 21 13:56

"can"

why?

imagine you own 100 mio USD of GPUs

please take a moment to think

you are some rich business man

you own 100 mio USD of GPUs

you will "move on"?

really?



Danno Ferrin @shemnon Mar 21 13:57

to a different coin.

assuming there are any GPU coins left at that point.



Sonia-Chen @Sonia-Chen Mar 21 13:57

from the largest GPU coin?

right

how many employees do you have?



Danno Ferrin @shemnon Mar 21 13:57

Or move on to ML.

Not a business owner.



Sonia-Chen @Sonia-Chen Mar 21 13:57

it's just a thought example

can't you imagine telling one of your managers "try all you can to keep the rewards flowing to my GPUs"?

and don't you think some smart guy really can have A LOT of ideas what "all you can" can be?

you are sure this is not possible, yes?

this won't happen

your story is: the honest businessman who owns 100 mio USD of GPUs will instruct his workers to take them all off the shelves, sell them on eBay, close down the datacenter, return the transformers and terminate the power delivery contracts.

my point is this: You need to think long and hard about who that owner of all these GPUs actually is

is it 100 Peter Salankis?


then you are safe!


is it Calvin Ayre?


then you are in BIG BIG trouble


that's a fact  
not FUD  
I have a question for you, quite important to me  
so a lot of people are saying "the ASIC" makers do all this FUD  
FUD FUD FUD  
but when you look at the recent medium post, by "Jon Stevens", titled "13 questions about Progpow"  
did you see that article?


 Danno Ferrin @shemnon Mar 21 14:01  
yes


 Linshi Sonia-Chen @Sonia-Chen Mar 21 14:01  
this article is a masterpiece of FUD  
do you realize that?  
or you see it as a "helpful" article?  
I am curious how you feel about it


 Danno Ferrin @shemnon Mar 21 14:02  
didn't read it too deeply. He had a lot of criticism but surprisingly came out in favor of PP.

 Linshi Sonia-Chen @Sonia-Chen Mar 21 14:02  
FUD is so interesting  
we all think it cannot affect us  
it's not worth reading it deeply, but in terms of what this article is: a marketing masterpiece, written by or paid by Nvidia  
they do this all the time  
maybe it matters, maybe not  
but when I hear "ASIC ... FUD..." I'm laughing  
we are just a bunch of engineers  
and the real FUD pieces like that one, people cannot even tell  
so yeah  
that's how it is  
if Progpow comes, it will empower the wrong people. hopefully it works out!  
the fork itself should not be a big problem I think, I said that. I don't believe ASIC makers will work on a contentious fork.  
I asked around.  
we don't, Bitmain won't, etc.

 Danno Ferrin @shemnon Mar 21 14:05  
this line of discussion underlines why I think your advocacy was ineffective. Rather than staying engaged on the technical merits you focus on who funded it, that it was FUD, how I am a naive developer, etc.


 Linshi Sonia-Chen @Sonia-Chen Mar 21 14:05  
you need to think yourself  
FUD is what you cannot detect, by definition  
Hudson asked me "write a paper how mining on GPUs benefits insiders"  
too hard!


 Danno Ferrin @shemnon Mar 21 14:06  
No, Hudson was prodding you to focus on the technical issues.

 Linshi Sonia-Chen @Sonia-Chen Mar 21 14:06  
but they are minor here. Progpow should be safe. Like Kristy says it looks like Ethereum+  
we published enough. the rest is up to the ETH community  
I don't think we can contribute much more quality thoughts  
(about Progpow)  
if something interests you specifically, feel free to ask  
we will definitely be around. this is all just starting. if Progpow is active in 2020 it will get very interesting.  
the ETH community will get stronger from this

 Danno Ferrin @shemnon Mar 21 14:15  
thanks, talk to you later.


 Linshi Sonia-Chen @Sonia-Chen Mar 22 13:16  
if and when you are interested in talking about money laundering, scammers, secret optimizations, unsellable chips etc. let me know

 Danno Ferrin @shemnon Mar 22 13:17  
not really, but if I change my mind I know who to ask now.


 Linshi Sonia-Chen @Sonia-Chen Mar 27 11:40  
hi Danno, how are you?  
have you heard of the randomness in Progpow?

 Danno Ferrin @shemnon Mar 27 12:55  
Yes. What is the concern?

 Linshi Sonia-Chen @Sonia-Chen Mar 27 13:03  
no concern. just wondering why it's in there. "random" is mentioned 22 times in EIP 1057. What do you believe is the function of the randomness?

 Danno Ferrin @shemnon Mar 27 13:06  
KISS99 provides the deterministic randomness (kind of an oxymoron). It sets the lane swapping, the computation "program" and some other parts of the computation.


The function is to create a widely varying setup for the hash function. Since it is deterministic it is really pseudorandom, but there is no need to be pedantic in the spec since the function providing the pseudorandom number generation is clear and in the open.


 Linshi Sonia-Chen @Sonia-Chen Mar 27 13:08  
yeah but why is the random program there at all?


 Danno Ferrin @shemnon Mar 27 13:08  
so that it has greater variation at each Progpow period. A simple incrementor won't provide the needed variety of evaluation patterns.


 Linshi Sonia-Chen @Sonia-Chen Mar 27 13:10  
"the random program changes every PROGPOW\_PERIOD blocks to ensure the hardware executing the algorithm is fully programmable"  
what does that mean?


 Danno Ferrin @shemnon Mar 27 13:11


 Yes, the spec even calls it out. perhaps it could have been phrased "the program that is derived from a pseudorandom sequence" basically it makes sure that whatever hardware it is running on is basically a GPU. Traditional mining ASICs could deal with fixed math, but the program derived from the pseudorandom sequence ensures that each lane has to have access to all the functions to be efficient.


 Sonia-Chen @Sonia-Chen Mar 27 13:13  
the program is not turing complete  
no jumps, no loops, just forward arithmetic and read-only memory accesses


 Danno Ferrin @shemnon Mar 27 13:13  
right, it's a calculation. Lack of pendantic spec is not a technical flaw.


 Sonia-Chen @Sonia-Chen Mar 27 13:14  
an asic would pipeline this, just with more mux inside


 Danno Ferrin @shemnon Mar 27 13:15  
correct. But at what point does the ASIC look like a GPU in architecture?


 Sonia-Chen @Sonia-Chen Mar 27 13:15  
not at all. but I understand the "random" to you is basically OK the way it is.  
for an asic it has no meaning


 Danno Ferrin @shemnon Mar 27 13:16  
it's a calculation to determine what calculations to perform.


 Sonia-Chen @Sonia-Chen Mar 27 13:17  
EIP 1057 seems to be written with the claim that the randomness increases asic resistance, or forces "full programmability" (that's what it says)  
if it's clear that that is not the case then that's fine


 Danno Ferrin @shemnon Mar 27 13:18  
as in you can program what calculations are to be done. programmable != turing complete.  
bitcoin's redeem scripts are programmable, but also not turing complete.


 Sonia-Chen @Sonia-Chen Mar 27 13:19  
yes, but as I said an asic would pipeline this, a mux based dataflow controlled by an instruction decoder, so it makes no difference to an asic at all.  
it seems that is understood and ok, at least with you. great! :)


 Danno Ferrin @shemnon Mar 27 13:20  
more circuits, more die size, less efficiency. It's not that progrpow makes asics impossible, just reduces the efficiency gains.


 Sonia-Chen @Sonia-Chen Mar 27 13:20  
we might even gain efficiency because we can optimize that dataflow better than a gpu, but ok  
the "programmability" may make some people believe it "has to be" a gpu somehow  
you helped me a lot, thanks!


 Danno Ferrin @shemnon Mar 27 13:21  
not a hardware engineer, but it has to do with the number of functional units that would be needed.


 Sonia-Chen @Sonia-Chen Mar 27 13:21  
well  
to an asic the random program makes no difference  
it's not "random", because it would be a pipelines, with mux and instruction decoder  
if that is clear, all is good


 Danno Ferrin @shemnon Mar 27 13:23  
right. pseudorandom. Predictable from a seed but otherwise not predictable from the output values. deterministic


 Sonia-Chen @Sonia-Chen Mar 27 13:23  
it doesn't matter to an asic. just some logic


 Danno Ferrin @shemnon Mar 27 13:23  
same with software.


 Sonia-Chen @Sonia-Chen Mar 27 13:24  
some ops are slow, like div, but largely it's still a simple pipeline  
it's not programmable, it can only execute all variations of the random program, decode and calculate  
I don't think anyone has started with a design yet, but we might even gain efficiency over a GPU thanks to that program. I will investigate a little.

 Sonia-Chen @Sonia-Chen May 03 08:39  
hi Danno! hope this finds you well. Has noone filled you in on the latest from the progpow frauds yet? Calvin is suing Vitalik, and gave Kristy new directions at their Toronto conference (and tweeted about it, since deleted). The tweet said kristy is "porting" her stuff from eth to bsv, whatever that means.  
since you don't want to take me serious, maybe you can talk to Trenton van epps, he has been doing some investigations  
I don't know what Trenton found out and I am not in touch with him, but I know he has actually been thinking rather than blindly following fraudulent agendas...  
good luck!

 Sonia-Chen @Sonia-Chen Aug 24 20:42  
hey Danno, sorry to bother you... But since you are still championing for the money launderers  
<https://www.reddit.com/r/ethereum/comments/cusqv/>  
I know you are new to Ethereum, but please try to get in touch with the foundation, or vitalik. they know what is going on but I guess noone knows what to do... good luck!

 Danno Ferrin @shemnon Aug 25 12:28  
Sonia, please stay away.

 Sonia-Chen @Sonia-Chen Sep 15 22:24  
<https://coingeek.com/kristy-leigh-minehan-bitcoin-sv-is-treating-miners-right-video/>  
can you give commentary to the fact that you are inviting a major BSV miner to help with Ethereum mining?

 Sonia-Chen @Sonia-Chen Sep 24 05:07  
danno, apologies already about "negativity" and all that stuff... it's not true. it's just the power of inconvenient truths. I do not want to tweet this to not give BSV any publicity, but could you please read this?  
<https://svpool.com/business/bigger-blocks-will-make-the-whole-mining-network-raise-its-game/>  
it's not third-degree, or association, or anything. please read for yourself. BSV will go to 0, but ETH will not.  
klm is a major BSV figure and has been for a long time. scamming is her profession. sorry about that.  
wish you good luck!



Click here to type a chat message. Supports GitHub flavoured markdown.



