

Forum:[Hack Forums](#)

Thread: [Calling out "Bitcoin Core Contributor" MeshCollider regarding Bitcoin Cash](#)

Orgy - September 12, 2017, 1:37 pm

Hey MeshCollider, since you refused to clarify in that other thread, I thought I'd see if you wouldn't mind clarifying here.

At one point, you called Bitcoin Cash:

(Sep 10, 2017 06:05 AM)MeshCollider Wrote: [\[CITE\]](#) a fail

Since then, I've tried to get you to back up this claim. I found out that you consider a coin to be a fail if it has:

(Sep 10, 2017 01:10 PM)MeshCollider Wrote: [\[CITE\]](#) lack of replay protection and even basic ability to send transactions on the day of release

Though Bitcoin Cash had both of these. After you realized that those claims were wrong, you moved on to:

(Sep 10, 2017 04:49 PM)MeshCollider Wrote: [\[CITE\]](#) I'm thinking about the trustworthiness and quality of the 'developers' of cash and it's code, code which is hacked together with a much lower standard of QA, test and review compared to core. That's why they had technical issues, and that's why I'm calling it messy.

Now that you've shifted your qualifications for a coin to be

(Sep 10, 2017 06:05 AM)MeshCollider Wrote: [\[CITE\]](#) a fail from your previous requirements to now this new slew of slander, can you please elaborate on how Bitcoin Cash, a coin with multiple client/node implementations, has "hacked-together code"? I understand that you probably meant Bitcoin ABC, which is only one of the single client/node implementations for Bitcoin Cash. If that's the case, can you please explain why you think Bitcoin ABC is hacked together, and which technical issues the "hacked together code" of ABC caused for Bitcoin Cash?

SUI-3183372 - September 12, 2017, 1:43 pm

Hmm maybe MeshCollider.... HMMMM....

Maybe this is a chance for you to clearly state your position

Ravioli - September 12, 2017, 3:35 pm

yeah i saw this dude's replies on that thread and he seemed pretty ignorant tbh, let's see what he has to say.

Orgy - September 12, 2017, 4:49 pm

(Sep 12, 2017 03:55 PM)James! Wrote: [\[CITE\]](#) Isn't this the guy that did omnicoin, which failed btw?

Yes, but I'm not sure its fair to call that a failure. That was more of an HF experiment and it went well as far as experiments go. Of course you can't expect it to take off if it's solely marketed on HF, for HF.

Vana - September 12, 2017, 4:50 pm

I sent him a PM asking for a response on that thread - it was read and ignored.

grady - September 12, 2017, 4:52 pm

(Sep 12, 2017 04:49 PM)Orgy Wrote: [\[CITE\]](#) Yes, but I'm not sure its fair to call that a failure. That

was more of an HF experiment and it went well as far as experiments go. Of course you can't expect it to take off if it's solely marketed on HF, for HF.

Ye, the "success" of OMC pretty much required wide adoption within HF, but there's really no market for its use.

It was just 100x better to use BTC at that point, instead of wasting time & money exchanging for OMC.

Orgy - September 12, 2017, 4:54 pm

(Sep 12, 2017 04:50 PM)Vana Wrote: [\[CITE\]](#) I sent him a PM asking for a response on that thread - it was read and ignored.

He read my PMs a few times, but only responded by changing the -rep he left me.

Admittedly I have him on ignore -- I want him to reply publicly. You'd think a guy that brags about tiny (and [questionable](#)) commits to the bitcoin core repo would be totally excited to come back up his claims

You still on the Core side btw?

Omniscient - September 13, 2017, 6:40 am

Why bother calling him out so publicly? Are you really that butthurt he called Bitcoin Cash a fraud? Does his opinion matter so much to you?

And I'm not sure we can call Bitcoin Cash a success yet either.

Orgy - September 13, 2017, 7:03 am

(Sep 13, 2017 06:40 AM)Omniscient Wrote: [\[CITE\]](#) Why bother calling him out so publicly? Because he made his claims in public.

(Sep 13, 2017 06:40 AM)Omniscient Wrote: [\[CITE\]](#) Are you really that butthurt he called Bitcoin Cash a fraud? Does his opinion matter so much to you?

If it weren't for the fact that he of all people should know better, I wouldn't care. But he's well known around here for the development of omnicoïn and the HF API, so I hold him to a higher standard. Or at least I did. If he's going to make these sorts of claims, I certainly expect him to back them up or admit that he was just parroting shit and didn't actually have idea what he was saying.

(Sep 13, 2017 06:40 AM)Omniscient Wrote: [\[CITE\]](#) And I'm not sure we can call Bitcoin Cash a success yet either.

We absolutely can.

DevSquad - September 13, 2017, 7:06 am

<https://hackforums.net/private.php?action=send> seems to be a function!

Orgy - September 13, 2017, 7:13 am

(Sep 13, 2017 07:06 AM)DevSquad Wrote: [\[CITE\]](#) <https://hackforums.net/private.php?action=send> seems to be a function!

Try reading the thread:

<https://hackforums.net/showthread.php?tid=5716409&pid=55841192#pid55841192>
<https://hackforums.net/showthread.php?tid=5716409&pid=55841209#pid55841209>

Vana - September 13, 2017, 11:29 am

(Sep 13, 2017 06:40 AM)Omniscient Wrote: [\[CITE\]](#) And I'm not sure we can call Bitcoin Cash a success yet either.

Why would you call it anything but a success?

(Sep 12, 2017 04:54 PM)Orgy Wrote: [\[CITE\]](#) You still on the Core side btw?
I have holdings in both coins :)

Orgy - September 13, 2017, 11:30 am

(Sep 13, 2017 11:29 AM)Vana Wrote: [\[CITE\]](#) Why would you call it anything but a success?
oooooh thats smooth

Zack Fair - September 13, 2017, 12:01 pm

I don't see him responding, would be surprised. You called him out multiple times on his own thread, pushing him to reply and he just ignored it lol.

Orgy - September 13, 2017, 12:07 pm

(Sep 13, 2017 12:01 PM)Zack Fair Wrote: [\[CITE\]](#) I don't see him responding, would be surprised. You called him out multiple times on his own thread, pushing him to reply and he just ignored it lol. yeah kind of pathetic someone like that cant back up their claims. i used to have quite the respect for him, too, because i thought he was someone who knew his shit. between the hf api and omnicoin i thought he was pretty competent. but now not even the nuts to come in and say "you know what guys i made some claims that i just heard somewhere else and didnt actually look into but i was wrong, my bad"

tbh if it was almost anyone else i probably wouldnt have made this thread. there's very few people here that i deem worthy of respect and he was one of them. i guess that's why it bothers me so much.

meh oh well. ima keep the thread bumped till omni gets pissed at me enough to close it or till messcollider gets in here.

SUI-3183372 - September 13, 2017, 1:21 pm

Well, he was just here but opted not to post. May not be able to backpedal hard enough. Not easy to back pedal to that degree.

FamousHater - September 13, 2017, 1:22 pm

wonder what omni thinks about this since after all he had mesh help with the API

Orgy - September 13, 2017, 1:23 pm

(Sep 13, 2017 01:21 PM)Previously Known As.... Wrote: [\[CITE\]](#) Well, he was just here but opted not to post. May not be able to backpedal hard enough. Not easy to back pedal to that degree.
HE'S REPLYING!!!!

hopefully he actually explains things in his own words instead of linking to blogs and articles.

FamousHater - September 13, 2017, 1:27 pm

(Sep 13, 2017 01:23 PM)Orgy Wrote: [\[CITE\]](#) HE'S REPLYING!!!!

hopefully he actually explains things in his own words instead of linking to blogs and articles.no

User(s) browsing this thread: Donald Trump Jr., FamousHater*, madTRiiKs*, MazI*, Orgy*, SIMAAS, Toph*, Vana*

Orgy - September 13, 2017, 1:28 pm

(Sep 13, 2017 01:27 PM)FamousHater Wrote: [\[CITE\]](#) no

User(s) browsing this thread: Donald Trump Jr., FamousHater*, madTRiiKs*, Mazl*, Orgy*, SIMAAS, Toph*, Vana*

You don't show up as browsing when you're making a reply.

Also he's been working on that reply for over 10 minutes now

Prawnster - September 13, 2017, 1:28 pm

(Sep 13, 2017 01:22 PM)FamousHater Wrote: [\[CITE\]](#) wonder what omni thinks about this since after all he had mesh help with the API

I doubt Omni is too bothered, API seems to look great & that's probs the bit he cares about the most & the rest is just stuff that he doesn't have time to care about lol

?heshire - September 13, 2017, 1:29 pm

I love these threads. They just give me pure joy.

SIM-2015410 - September 13, 2017, 1:30 pm

Out of regard to the mutual respect we used to have for each other Orgy, I've changed my mind, and will respond. At first I had decided to ignore you because it was getting much too heated for a reasonable debate, there is no need for all the random insults ok?

Yes you're right, I was mostly referring to bitcoin-abc and electron cash, I wasn't aware of other clients at the time. And no, I'm not aware of technical issues which affected the network as a whole, I had in mind issues which only affected individual users, because I'm one of the top posters on the bitcoin stack exchange and witnessed the flood of support questions there first hand. I realise that a lot of issues have been fixed since release, but there was a lot of troubles splitting bitcoin and cash, with very little documentation, so many people were losing coins, and I'm still fairly sure that 2 way replay protection was only implemented after the fact, at the initial release there was only a form of 1-way replay protection by putting a specific message in a OP_RETURN output in the tx? EDIT: I just checked, it was the fact that replay protection was opt-in not compulsory that was the issue. Additionally a lot of code-stealing with ABC, things like them taking sipa's schnor signature aggregation code from libsecp256k1 and other commits to core, and using them without individual attribution (referring to this <https://github.com/Bitcoin-ABC/bitcoin-abc/issues/85>). Other thing I have a complain with is that electron cash is closed source (unless this was changed?).

So yes I apologise for potentially overgeneralizing the issues I thought cash had via ABC, and shouldn't have started a debate on a topic which we both clearly feel quite dedicated to (because you're clearly cash and I'm clearly core). But the ad hominem, insulting my contributions, and constant PM spam were a completely barrier to me wanting to discuss this further, hence my delay in reply. None of that contributes to a healthy discussion.

SIM-2015410 - September 13, 2017, 1:39 pm

Wow this thread is popular ?

Orgy - September 13, 2017, 1:40 pm

[snipped out irrelevant content in these quotes -- just focusing on arguments]

(Sep 13, 2017 01:30 PM)MeshCollider Wrote: [\[CITE\]](#) I realise that a lot of issues have been fixed since release, but there was a lot of troubles splitting bitcoin and cash, with very little documentation, so many people were losing coins,

I'm not sure how that's any sort of technical issue. Sounds like users of Bitcoin just don't understand how private keys work. The only "splitting" necessary was just importing your private key into a wallet that follows the bitcoin-cash chain, so I'm not really sure what sort of documentation is

needed for that. Perhaps Bitcoin needs to make users more aware of how their private keys work and what they're for.

(Sep 13, 2017 01:30 PM)MeshCollider Wrote: [\[CITE\]](#) and I'm still fairly sure that 2 way replay protection was only implemented after the fact, at the initial release there was only a form of 1-way replay protection by putting a specific message in a OP_RETURN output in the tx?

Forgive me for my lack of technical knowledge here, but what would a 2-way replay protection need? Upon release it was impossible to do any sort of replay attacks. You should know this because there would have been a shitload of people dicking around with it. Even if it didn't have replay protection (and it did) I don't see how that would be a failure on Cash's part.

(Sep 13, 2017 01:30 PM)MeshCollider Wrote: [\[CITE\]](#) Additionally, I've seen a lot of code-stealing with ABC, things like them taking sipa's schnor signature aggregation code from libsecp256k1 and other commits to core, and using them without individual attribution (referring to this <https://github.com/Bitcoin-ABC/bitcoin-abc/issues/85>

Actually if you look further into that, you'll very well see that daedalnix did indeed provide proper attribution as required by the MIT license that Bitcoin uses. You'll also find that it was actually maxwell of bitcoin core that was committing copyright infringement <https://github.com/bitcoin/bitcoin/pull/11318>

(Sep 13, 2017 01:30 PM)MeshCollider Wrote: [\[CITE\]](#) Other thing I have a complain with is that electron cash is closed source (unless this was changed?).
as far as i know it's always been open source.

(Sep 13, 2017 01:30 PM)MeshCollider Wrote: [\[CITE\]](#) So yes I apologise for potentially overgeneralizing the issues I thought cash had via ABC, and shouldn't have started a debate on a topic which we both clearly feel quite dedicated to (because you're clearly cash and I'm clearly core). But the ad hominem, insulting my contributions, and constant PM spam were a completely barrier to me wanting to discuss this further, hence my delay in reply. None of that contributes to a healthy discussion.

this is the one irrelevant thing i'll respond to about it. none of the pm spam and insults started until after you decided to start ignoring the questions.

by the way, which of these points you made are the technical issues you were referring to?the false claim about lack of replay protection

the false claim about copyright infringement

the false claim about electron cash (just one wallet available for BCC) being closed source

people didnt know how to import their bitcoin private key somewhere else

Vana - September 13, 2017, 1:41 pm

(Sep 13, 2017 01:30 PM)MeshCollider Wrote: [\[CITE\]](#) Other thing I have a complain with is that electron cash is closed source (unless this was changed?).

<https://github.com/fyookball/electrum>

It was never closed-source.

SIM-2015410 - September 13, 2017, 1:49 pm

(Sep 13, 2017 01:40 PM)Orgy Wrote: [\[CITE\]](#) Forgive me for my lack of technical knowledge here, but

what would a 2-way replay protection need? Upon release it was impossible to do any sort of replay attacks. You should know this because there would have been a shitload of people dicking around with it. Even if it didn't have replay protection (and it did) I don't see how that would be a failure on Cash's part.

2 way replay protection needs a way for cash transactions to be invalid on Bitcoin, and Bitcoin transactions to be invalid on cash. They added both of these in but left them opt-in until later, which is the issue, they should have been mandatory from the start.

Quote:as far as i know it's always been open source.

Ah yes sorry, I was thinking of the fact the person who distributes the Electron Cash binaries is anonymous, ("Jonald Fyookball") when signing the Electron Cash binaries. So if there was something malicious in them, the author will be anonymous and walk away safely.

Im just contrasting it against core, which on the other hand has a very open process for deterministic gitian building the source, signing and then being released with laanwj's key, Wladimir is the opposite of anonymous.

Orgy - September 13, 2017, 2:01 pm

(Sep 13, 2017 01:49 PM)MeshCollider Wrote: [\[CITE\]](#) 2 way replay protection needs a way for cash transactions to be invalid on Bitcoin, and Bitcoin transactions to be invalid on cash. They added both of these in but left them opt-in until later, which is the issue, they should have been mandatory from the start.

Nope. It was 2-way and mandatory from the start.

(Sep 13, 2017 01:49 PM)MeshCollider Wrote: [\[CITE\]](#) Ah yes sorry, I was thinking of the fact the person who distributes the Electron Cash binaries is anonymous, ("Jonald Fyookball") when signing the Electron Cash binaries. So if there was something malicious in them, the author will be anonymous and walk away safely.

Im just contrasting it against core, which on the other hand has a very open process for deterministic gitian building the source, signing and then being released with laanwj's key, Wladimir is the opposite of anonymous.

Again, I'm not sure how this is a technical issue. In fact it's really not even a Cash issue. Anyone can go fork an SPV client and build it and distribute it.

So, technical issues?

SIM-2015410 - September 13, 2017, 2:09 pm

(Sep 13, 2017 02:01 PM)Orgy Wrote: [\[CITE\]](#) Nope. It was 2-way and mandatory from the start.

Not according to this answer:

<https://bitcoin.stackexchange.com/a/56874/51948>

Orgy - September 13, 2017, 2:11 pm

(Sep 13, 2017 02:09 PM)MeshCollider Wrote: [\[CITE\]](#) Not according to this answer:

<https://bitcoin.stackexchange.com/a/56874/51948>

That answer's last edit was from before Bitcoin Cash even forked away... Hell look at the comments dude.

SIM-2015410 - September 13, 2017, 2:14 pm

(Sep 13, 2017 02:11 PM)Orgy Wrote: [\[CITE\]](#) That answer's last edit was from before Bitcoin Cash even forked away... Hell look at the comments dude.

Hmm you're right, so they must have fixed it by the day of the fork. Fair enough then, I apologise for

my confusion ?

Orgy - September 13, 2017, 2:16 pm

(Sep 13, 2017 02:14 PM)MeshCollider Wrote: [\[CITE\]](#) Hmm you're right, so they must have fixed it by the day of the fork. Fair enough then, I apologise for my confusion ?

So, Cash a failure? Technical issues? Anything else?

SIM-2015410 - September 13, 2017, 2:20 pm

(Sep 13, 2017 02:16 PM)Orgy Wrote: [\[CITE\]](#) So, Cash a failure? Technical issues? Anything else? I retract my comment on whether cash is a success or failure as that's very opinion based, I apologise for making such sweeping claims in the first place.

/Thread?

Orgy - September 13, 2017, 2:21 pm

(Sep 13, 2017 02:20 PM)MeshCollider Wrote: [\[CITE\]](#) I retract my comment on whether cash is a success or failure as that's very opinion based, I apologise for making such sweeping claims in the first place.

/Thread?

/Thread. Thanks.

SUI-3183372 - September 13, 2017, 2:23 pm

(Sep 13, 2017 02:11 PM)Orgy Wrote: [\[CITE\]](#) That answer's last edit was from before Bitcoin Cash even forked away... Hell look at the comments dude.

Paying attention to details is important.

Orgy - September 13, 2017, 2:27 pm

(Sep 13, 2017 02:23 PM)Previously Known As.... Wrote: [\[CITE\]](#) Paying attention to details is important.

Indeed but everything's all cleared up now. Hopefully in the future MeshCollider will do his own research instead of just blindly listening to the Core propaganda ;)

Anyway, closing this thread as I'm satisfied with its resolution. Thanks for coming out, everyone, and if any of you have any questions just PM me.