

Forum:[Hack Forums](#)

Thread: [MASSIVE - Bitcoin Block Reorg Attack](#)

shreder - March 18, 2023, 12:21 pm

I already warned, this is the result of 2 centralized mining pools controlling 51%+ of the network. They can do whatever the FUCK they want. You get what you f*cking deserve.

L shutting down their little spamming Monkey jpeg explorer due to reorg attack.

Quote:More sleuthing found that this was 100% a premeditated attempt to mine the degods block

@FoundryServices mined block
000000000000000000000000388f42000fa901c01f2bfae36042bbae133ee430e6485 which was then re-orged via a selfish mining attack

Notice 781276/781277/781278 all come at the same second

@AntPoolofficial / @ViaBTC clearly in cahoots on this

h/t @timechainord

shreder - May 25, 2023, 12:08 pm

As ordinals gaining traction, i expect miners to reorg more often.

shreder - May 25, 2023, 12:34 pm

Ordinals have the potential to earn more than block subsidies especially in the future for miners. Reorging blocks maybe profitable and Bitcoin has no security mechanisms against reorgs, unlike Ethereum which has absolutely finality after 2 epochs which makes blocks permanent.

There is no incentive not to reorg when it is more profitable to reverse blocks.

Bitcoin security is already falling apart now, it will be worse soon when its jenga tower security model collapses.

If reorgs are already common occurrence. Then they are incentivized to reorg day old blocks to double spend which would easily be worth more than their future revenue.

Warbiest - May 26, 2023, 2:42 pm

(May 25, 2023 12:58 PM)Focus Broken Wrote: [\[CITE\]](#) Reorging a previous block is less profitable than mining a new block, that's why the chain always advances forward instead of freezing.

Why would you tell your node to ignore the chain with the most staking weight if it is older than 2 epochs?

Except it's not profitable to reverse a block compared to mining a new block. Mining a new block guarantees rewards while mining a previous block risks creating an orphan unless you have >51% of the hashrate.

All of this do be sounding extremely finnick when ordinals are involved though, doesn't it?

shreder - May 26, 2023, 5:32 pm

(May 26, 2023 02:42 PM)Warbiest Wrote: [\[CITE\]](#) All of this do be sounding extremely finnick when ordinals are involved though, doesn't it?

Next year the block rewards will go from 6.25 to 3.125.

Let's assume the price stays the same miners just lost half their typical block subsidies. It makes reorgs that much more profitable, especially now with ordinals in the pictures that may be profitable to double-spend.

There are no consequences as we can see, literally, Bitcoin got rolled back block 781277 yet the community brushed it under the rug. So much for an immutable blockchain that is unchanging forever.?

There is literally NOTHING stopping another reorg from happening on Bitcoin.

Bullup - May 27, 2023, 4:29 am

(May 26, 2023 05:32 PM)shreder Wrote: [\[CITE\]](#) Next year the block rewards will go from 6.25 to 3.125.

Let's assume the price stays the same miners just lost half their typical block subsidies. It makes reorgs that much more profitable, especially now with ordinals in the pictures that may be profitable to double-spend.

There are no consequences as we can see, literally, Bitcoin got rolled back block 781277 yet the community brushed it under the rug. So much for an immutable blockchain that is unchanging forever.?

There is literally NOTHING stopping another reorg from happening on Bitcoin.

You contradict yourself, you start with the fact that block rewards are cut in half, price stays the same, and therefor lesser profits, but then mention that nothing will stop another reorg from happening, yet another reorg at that point would mean even lesser profit then advancing forward to new blocks, so answer why would people find a another reorg interesting to begin with?

I'm not keen on Bitcoin, more keen on Ethereum and some others these days, but your con-posts about bitcoin are missing a lot of logic, and your pro-posts about ethereum are also missing a lot of logic and most often contradict your con-posts about bitcoin, you are not the brightest i get that, but at least try not to contradict yourself so much and stop with the hate towards bitcoin, you don't want bitcoin to die anytime soon, it wouldn't mean anything good for ethereum either, because ethereum will then become #1 and that would essentially mean that crypto's entirely will just become a small niche for the next decade as it will take that much time for ethereum to gain brand awareness on the level that bitcoin currently has, and most likely more time than that because if Bitcoin now dies for any reason, the biggest brand in crypto, after all past scandals that happened and gave crypto a bad name, imagine what impact that would have on the name of crypto itself, Ethereum needs bitcoin to pull in new investors as Bitcoin is the gateway right now and will remain so for a long time to come, rather focus on facts only because you try to twist around a lot as well and that is just plain annoying.

Imagine Bitcoin dies tomorrow, huge scandal, people in crypto right now losing faith left and right as

the king has died, companies on the verge of investing in crypto will dismiss those plans, average joe's will laugh and say i told you so, overtime market keeps tanking as no new investors are coming in, people will lose faith in crypto as a whole, people will continue pulling out, crypto becomes a small digital niche, just like there are many digital niche's, there will be so few funds in the market that crypto isn't being taken seriously no more, and the few people left in crypto will realize that it will take at least a decade for crypto to gain some fame again, regardless of which crypto is #1 at that point.

Maybe gov's will use the technology at that point too create gov backed coins with small usage points, to blow the last candle out on the cake of victory they have and other cryptos which at that point have survived will then be back at 2014 times, used by criminals only but lets face it, exchanges are by that time already bought up by gov's or fully centralised and most criminals, just like now, will continue using cash instead.

We need Bitcoin, not for what bitcoin is, but what it represents, and the status that it has.

Ethereum needs Bitcoin to grow.

Crypto needs Bitcoin to grow.

Bitcoin gateways new investors towards alt coins.

Bitcoins gateways new developers towards blockchain.

Bitcoin is not perfect, but it's all we got right now in terms of brand awareness.

shreder - May 27, 2023, 9:39 am

(May 27, 2023 04:29 AM)Cryptomander Wrote: [\[CITE\]](#) You contradict yourself, you start with the fact that block rewards are cut in half, price stays the same, and therefor lesser profits, but then mention that nothing will stop another reorg from happening, yet another reorg at that point would mean even lesser profit then advancing forward to new blocks, so answer why would people find a another reorg interesting to begin with?

Current block rewards are 6.25 yet a reorg already happened. This displays that even in the current climate the block subsidies are not enough of a incentive to stop a reorg.

When you cut the block subsidies in half again, you just lost half your incentive to not be malicious. When ordinals pick up to the point where ETH nfts were in 2020 half a million multiple millions dollars. It will be highly profitable to double spend and potentially get hundreds of millions of dollars. Than your \$60k block subsidies.

There also is no long term consequences. The community didnt even condemn the miner, it was brushed off.