

Forum:[Hack Forums](#)

Thread: [Recently I've noticed a lot of people shit on PoS](#)

Mabylossus - July 27, 2021, 7:18 pm

Can someone explain to a legit newbie why PoS is apparently bad?

Why do people say that it's no different to the current money system? Any counter arguments to that?

SIM-964740 - July 27, 2021, 9:46 pm

simple... cause consensus is elite

shreder - July 28, 2021, 12:14 am

There are many different PoS protocols that take different approaches to the "nothing at stake" problem, and it's not a problem anymore. Idiots claim "heRe's HOw yOU CAN hACK ANY POS bLOCKChaln", Don't trust... Verify. Hack a PoS blockchain then come back with proof, until then everything they say is garbage. Hack any of the top 10 PoS chains by market cap with your little "tutorial" within 24 hours. Otherwise don't bother posting.

shreder - July 28, 2021, 12:38 am

"heRe's HOw yOU CAN hACK ANY POS bLOCKChaln"

Hack any PoS blockchain in the top 20 by MC within the next 24hrs. Any further reply without verifiable proof is admittance that you cant do it. Dont try to stall, I already debunked it in my first comment. Show us your hax little man.

Tesseract.mk - July 28, 2021, 12:49 am

(Jul 28, 2021 12:14 AM)shreder Wrote: [\[CITE\]](#) There are many different PoS protocols that take different approaches to the "nothing at stake" problem, and it's not a problem anymore. Idiots claim "heRe's HOw yOU CAN hACK ANY POS bLOCKChaln", Don't trust... Verify. Hack a PoS blockchain then come back with proof, until then everything they say is garbage. Hack any of the top 10 PoS chains by market cap with your little "tutorial" within 24 hours. Otherwise don't bother posting. Are you gonna make another gif? I miss the last one lmao

shreder - July 28, 2021, 12:56 am

(Jul 28, 2021 12:49 AM)Tesseract.mk Wrote: [\[CITE\]](#) Are you gonna make another gif? I miss the last one lmao
"heRe's HOw yOU CAN hACK ANY POS bLOCKChaln" - broke

I knew he was autistic but dam, I guess hes moving further down the spectrum.

x_x - July 28, 2021, 12:57 am

[shreder](#) why is your title "shreded" and not "shredded"?

shreder - July 28, 2021, 1:17 am

Cant even read simple instructions even after I dumbed it down for him. "Hack any PoS blockchain in the top 20 by MC within the next 24hrs." Radix launches tomorrow also maybe your cheat file works on dPoS?

(Jul 28, 2021 12:57 AM)x_x Wrote: [\[CITE\] shredder](#) why is your title "shreded" and not "shredded"? Because people cant handle a second D.

But OP you seem to be a smart guy. I debunked his "hOw tO haCk aNy poS bLockCHain" in singular post. Its clear as day from his attempts to derail or change subject that he cant do any "hacking". You've probably realized by now that all the hate against PoS are unfounded. Broke will continue to stall despite given explicit instruction. And with each stall, it only displays its inability to prove otherwise.

SeekHelp - July 28, 2021, 3:56 am

(Jul 28, 2021 12:16 AM)Focus Broken Wrote: [\[CITE\]](#) What are some different PoS protocols and how did they solve the problem?

i thought this was a good question.... ?

Mainly here to read Focus Broken vs shredder. Always good banter.

Tesseract.mk - July 28, 2021, 4:14 am

(Jul 28, 2021 03:56 AM)SeekHelp Wrote: [\[CITE\]](#) i thought this was a good question.... ?

Mainly here to read Focus Broken vs shredder. Always good banter.

Yeah, shredders signature was hilarious last time, I died when I saw it haha.

OliverSc - July 28, 2021, 4:23 am

(Jul 27, 2021 11:08 PM)Focus Broken Wrote: [\[CITE\]](#) Proof of stake is conceptually broken due to the "nothing at stake" problem. Here's how you can hack any proof of stake blockchain:Own 100 coins at block height 500 and stake them on chain A

Sell 100 coins at block height 510 on chain A

Create chain B by staking a new history of blocks 500-511, but remove the transaction from block 510 where you already spent your money.

So when someone's node is validating block 511... how do they know whether or not to stake on chain A or chain B? Both are equally valid according to the protocol's rules, so they can't tell the counterfeit history apart from the honest history.

Additional to this, PoS by its nature is a centralized mechanism compared to proof of work.

Bitcoin was born under very unique circumstances, managed to survive, imagine that for 1.5 years from its launch it didn't even have a price, so you can understand many things about coin distribution.

On the other hand, all the altcoins was brutally bought from whales, devs premined/minted coins for themselves and the coin distribution sucks. So if you imagine that you have a blockchain where like 1000 members own the 60% of the coins, it's fairly obvious that as they stake, they "rule" the blockchain and it's completely centralized.

Same happens with every new project, even if technologically seems "perfect", whales will jump on the project with billions and will hold over 50% of the coins.

Centralized shitcoins, centralized shitcoins everywhere.

shredder - July 28, 2021, 6:06 am

"hERe's How you CAn hack aNY pROOF oF STAkE BloCkChAIN"

Instruction: Hack any PoS blockchain in the top 20 by MC within the next 24hrs. Obviously he can't do it, that's why he's beating around the bush.

SeekHelp - July 28, 2021, 6:12 am

(Jul 28, 2021 06:06 AM)shreder Wrote: [\[CITE\]](#) "hERe's How you CAn hack aNY pROOF oF STAkE BloCkChAIN"

Instruction: Hack any PoS blockchain in the top 20 by MC within the next 24hrs. Obviously he can't do it, that's why he's beating around the bush. Do you mean he cannot hack it himself or nobody at all can?

shreder - July 28, 2021, 6:13 am

(Jul 28, 2021 06:12 AM)SeekHelp Wrote: [\[CITE\]](#) Do you mean him personally or nobody at all can? He's the one who said "Here's how you can hack any proof of stake blockchain" so why not try out his cheats.

SeekHelp - July 28, 2021, 6:16 am

(Jul 28, 2021 06:13 AM)shreder Wrote: [\[CITE\]](#) He's the one who said "Here's how you can hack any proof of stake blockchain" so why not try out his cheats.

You seem to be avoiding the question, im asking if somebody else can hack it based on what Focus Broken has explained?

shreder - July 28, 2021, 6:19 am

It has free will to try his "hack" on any PoS blockchain in the top 20 by MC within the next 24hrs. I have given you many options by opening it to your own personal choice of what you want to "hack", if one doesn't work you can try the next. I wouldn't want to limit you in case your "hack" doesn't work.

18 hours remaining in this challenge can broke do it?

(Jul 28, 2021 06:16 AM)SeekHelp Wrote: [\[CITE\]](#) You seem to be avoiding the question, im asking if somebody else can hack it based on what Focus Broken has explained?

He's the one who said "Here's how you can hack any proof of stake blockchain" so why not try out his cheats.

No one is avoiding the question, I answered it sorry you don't understand.

Marvelous - July 28, 2021, 6:29 am

(Jul 28, 2021 06:16 AM)SeekHelp Wrote: [\[CITE\]](#) You seem to be avoiding the question, im asking if somebody else can hack it based on what Focus Broken has explained?

If it could be done it would have been done. We are literally dealing with millions of dollars of semi untraceable money. The incentive is there..

shreder - July 28, 2021, 6:53 am

(Jul 28, 2021 06:45 AM)Focus Broken Wrote: [\[CITE\]](#) You are framing it the wrong way: If PoS could have been done, it would have been done. The invention of PoW was the innovation that made decentralized currency possible since it solves the double spending problem by attaching a cost to creating counterfeit history B that must be greater than the cost of creating honest history A.

This is why [shreder](#) can't name a single PoS blockchain that exists: If PoS worked, it would have already existed before PoW.

Why would I need to name a single PoS blockchain, I'm making this flexible and EASY for you. Any of the coins in the top 20 market cap that are PoS to use your "hacks" on within 24 hours. If I name a single PoS blockchain I don't want to limit you, you can pick and choose any PoS in the top 20. If your "hacks" don't work on one you can do another and it'll still count. I'm making it as easy as it can be, yet you're still stalling. Only 17 hours remaining now.

(Jul 27, 2021 11:08 PM)Focus Broken Wrote: [\[CITE\]](#) Proof of stake is conceptually broken due to the "nothing at stake" problem. Here's how you can hack any proof of stake blockchain: Own 100 coins at block height 500 and stake them on chain A

Sell 100 coins at block height 510 on chain A

Create chain B by staking a new history of blocks 500-511, but remove the transaction from block 510 where you already spent your money.

So when someone's node is validating block 511... how do they know whether or not to stake on chain A or chain B? Both are equally valid according to the protocol's rules, so they can't tell the counterfeit history apart from the honest history.

shreder - July 28, 2021, 7:03 am

(Jul 28, 2021 06:58 AM)Focus Broken Wrote: [\[CITE\]](#) Don't make it flexible and easy for me. Choose your champion and let me slay him. Is it Binance Coin?

More or less sums up the thread, despite making it flexible and easy, broke still cannot produce any results. Don't worry you still have about 17 hours.

(Jul 27, 2021 11:08 PM)Focus Broken Wrote: [\[CITE\]](#) Here's how you can hack any proof of stake blockchain:

shreder - July 28, 2021, 7:25 am

hEre's HOw you CaN hack aNY ProoF oF sTake bLOckchAIn now he says they don't exist. LMAO, the delusion.

(Jul 27, 2021 11:08 PM)Focus Broken Wrote: [\[CITE\]](#) Here's how you can hack any proof of stake blockchain:

(Jul 28, 2021 07:22 AM)Focus Broken Wrote: [\[CITE\]](#) proof of stake blockchains don't exist

shreder - July 28, 2021, 7:29 am

We are witnessing a hilarious delusional episode from broke. First, it explains how to hack a PoS blockchain then it says they do not exist after getting embarrassed.

(Jul 27, 2021 11:08 PM)Focus Broken Wrote: [\[CITE\]](#) Here's how you can hack any proof of stake blockchain:

(Jul 28, 2021 07:22 AM)Focus Broken Wrote: [\[CITE\]](#) proof of stake blockchains don't exist

OliverSc - July 28, 2021, 7:38 am

It's funny how Focus replies with facts and shreder just stuck quoting the same thing again and again, seems like you can't see the wood for the trees

shreder - July 28, 2021, 7:42 am

Still doesn't change the fact that you can't hack any PoS blockchain made apparent by your lack of verifiable proof of such. Fact is that you can't do it, it's been 7 hours since and you have been able

to do so. I'm still waiting. I predict they'll just keep repeating nonsense over and over stalling. Their next comments will contain no evidence of any PoS blockchain in the top 20 MC being "hacked" within 24hours. Scroll down to see.

shreder - July 28, 2021, 7:55 am

Deluded here wants us to just trust what he says. You need to PROVE your claim. As i predicted in another post broke cannot put forth any evidence of such. And has yet to use his cheats to hack any PoS blockchain. He'll continue to post while trying to his best to redirect or shy away from providing evidence that he has hacked any PoS blockchain within the last 24 hours.

shreder - July 28, 2021, 7:59 am

(Jul 28, 2021 07:57 AM)Focus Broken Wrote: [\[CITE\]](#) I claimed PoS blockchains don't exist, you can't [prove a negative](#). The burden of proof lies on you, the person claiming that PoS blockchains exist. Why would you need to prove a negative, you are the one who said you can hack any PoS blockchain, go ahead and prove it the burden of proof lies on you. As I predicted clearly in the previous post he will redirect the question. He will continue to post nonsense or attempt to redirect the question as he cannot hack any PoS blockchain which he stated he could.

Maskin - July 28, 2021, 8:04 am

If PoS don't exist, then it can't be hacked or have any flaws.

This is what I learned today woop woop

shreder - July 28, 2021, 8:12 am

(Jul 28, 2021 08:04 AM)Ocarina Wrote: [\[CITE\]](#) If PoS don't exist, then it can't be hacked or have any flaws.

This is what I learned today woop woop

But but but I can hack it trust me watch me hack it in 3 simple steps.

Maskin - July 28, 2021, 8:20 am

(Jul 28, 2021 08:12 AM)shreder Wrote: [\[CITE\]](#) But but but I can hack it trust me watch me hack it in 3 simple steps.

Both of you confuse me sometimes ?

It's very entertaining though.

diesel - July 28, 2021, 8:25 am

(Jul 27, 2021 11:08 PM)Focus Broken Wrote: [\[CITE\]](#) Proof of stake is conceptually broken due to the "nothing at stake" problem. Here's how you can hack any proof of stake blockchain:Own 100 coins at block height 500 and stake them on chain A

Sell 100 coins at block height 510 on chain A

Create chain B by staking a new history of blocks 500-511, but remove the transaction from block 510 where you already spent your money.

So when someone's node is validating block 511... how do they know whether or not to stake on chain A or chain B? Both are equally valid according to the protocol's rules, so they can't tell the counterfeit history apart from the honest history.

Has this ever been addressed by Vitalik and co? What's their explanation? Seems too obvious to ignore....

shreder - July 28, 2021, 8:31 am

(Jul 28, 2021 08:25 AM)diesiel Wrote: [\[CITE\]](#) Has this ever been addressed by Vitalik and co? What's their explanation? Seems too obvious to ignore....
Why would they address it? According to him it doesn't exist.

Grimeta - July 28, 2021, 8:31 am

(Jul 28, 2021 04:23 AM)OliverSc Wrote: [\[CITE\]](#) Additional to this, PoS by its nature is a centralized mechanism compared to proof of work.

Bitcoin was born under very unique circumstances, managed to survive, imagine that for 1.5 years from its launch it didn't even have a price, so you can understand many things about coin distribution.

On the other hand, all the altcoins were brutally bought from whales, devs premined/minted coins for themselves and the coin distribution sucks. So if you imagine that you have a blockchain where like 1000 members own the 60% of the coins, it's fairly obvious that as they stake, they "rule" the blockchain and it's completely centralized.

Same happens with every new project, even if technologically seems "perfect", whales will jump on the project with billions and will hold over 50% of the coins.

Centralized shitcoins, centralized shitcoins everywhere.
So if Bitcoin migrated to PoS it'd be alright?

OliverSc - July 28, 2021, 8:34 am

(Jul 28, 2021 08:31 AM)Grimeta Wrote: [\[CITE\]](#) So if Bitcoin migrated to PoS it'd be alright? No it wouldn't be alright. It would be way more centralized than what it is right now.

Imagine that the community (both miners and nodes) don't vote in order to increase the blocksize or increase the blocktime cause they want a small-size Decentralized blockchain in order for everyone to be part of it.

OliverSc - July 28, 2021, 9:17 am

(Jul 28, 2021 08:50 AM)Focus Broken Wrote: [\[CITE\]](#) There's no difference between PoW and PoS in regards to creating an invalid block, miners/stakers "vote" on transaction ordering only.
I said that btc community tries their best to keep btc as decentralized as possible, changing pow to pos make it less decentralized due to the mechanism itself.

Omniscient - July 28, 2021, 7:55 pm

Until I see a top 10 PoS blockchain hacked because it is PoS. Then it's all Bullshit. It's like saying that you can hack any PoW blockchain with a 51% attack. One thing is theory the other is application. If I shut down every Bitcoin mining server in the world I could steal all Bitcoin. Dumb ass shit.

btw [shreder](#) put Focused Clown on your ignore list. Reading his posts is just painful. Save yourself the headache.

Instructions to hack any PoW.

1. DDoS all miners
2. Setup your own miners
3. Create new chain and steal all crypto.

Look, I can make idiotic instructions too.

Quote:No it wouldn't be alright. It would be way more centralized than what it is right now.

Nope. Just look at the mining pools. Five of them represent 70% of the hash rate. If just 3 of them colluded they could take over Bitcoin. How is that less centralized than PoS?

Quote:I said that btc community tries their best to keep btc as decentralized as possible

Community trying its best is not the same as actually fully 100% decentralized. By that definition, then PoS are also fully decentralized because those communities do their best to keep it so.

Marvelous - July 31, 2021, 11:53 am

(Jul 28, 2021 08:31 AM)Grimeta Wrote: [\[CITE\]](#) So if Bitcoin migrated to PoS it'd be alright? Bitcoin doesn't do upgrades. It took forever to get taproot and its a small upgrade. Lmao.

OliverSc - July 31, 2021, 11:58 am

(Jul 31, 2021 11:53 AM)Marvelous Wrote: [\[CITE\]](#) Bitcoin doesn't do upgrades. It took forever to get taproot and its a small upgrade. Lmao.

Yeah bitcoin doesn't have 1 team that rules the network and it takes time for the whole community to vote for an upgrade, you're completely right, that's how a decentralized network works. Plus bitcoin has already whatever it needs in order to be (and it is) the best network worldwide. Most secure, most decentralized, honest coins.

P.S. Imagine saying that taproot is a small upgrade.

Marvelous - July 31, 2021, 12:11 pm

(Jul 31, 2021 11:58 AM)OliverSc Wrote: [\[CITE\]](#) Yeah bitcoin doesn't have 1 team that rules the network and it takes time for the whole community to vote for an upgrade, you're completely right, that's how a decentralized network works.

P.S. Imagine saying that taproot is a small upgrade.

Imagine if ETH had to do what BTC has to do to get an upgrade implemented. Kinda hard to make a decentralized world computer like that.

Imagine BTC trying to be something it's not. BTC is a digital gold and nothing more.

OliverSc - July 31, 2021, 12:14 pm

(Jul 31, 2021 12:11 PM)Marvelous Wrote: [\[CITE\]](#) BTC is a digital gold and nothing more. If you believe that you didn't understand anything about bitcoin so it'll be like me talking to a wall.

Once you realise what bitcoin is, we can have a conversation.

SUI-3183372 - July 7, 2022, 12:31 pm

(Jul 7, 2022 12:08 PM)Focus Broken Wrote: [\[CITE\]](#) No one in this thread ever gave a single example of a Proof of Stake chain existing.

What do you mean by this?

Are you stating that current [self-proclaimed] PoS chains lack a quality that you consider fundamental to 'exist' or be labeled a 'chain'?

SUI-3183372 - July 7, 2022, 2:00 pm

(Jul 7, 2022 01:11 PM)Focus Broken Wrote: [\[CITE\]](#) I'm stating there's no way to have nodes with alternate staking histories to ever come to consensus without a centralized party deciding one for them. A chain history that says I own 100% of the coins is just as valid as a chain history that says you own 100% of the coins, there's no actual "proof" involved to act as a tiebreaker. It's basically a circular reference problem: Ownership of coins can't be used to determine who owns coins.

I went into more detail in this thread: <https://hackforums.net/showthread.php?tid=6162671>
I don't believe that this can be solved. However, I do think that a threshold exists where you can have an acceptable level of resistance against this issue. My concern is employing this acceptable level of resistance in a decentralized manner (and ideally not in an overly complicated manner either). I don't think we're ever going to have that perfect PoS chain that perfectly solves this issue, I'm just looking for the ones that can do so in a very acceptable manner.

Migos - July 9, 2022, 11:42 am

(Jul 27, 2021 11:08 PM)Focus Broken Wrote: [\[CITE\]](#) Proof of stake is conceptually broken due to the "nothing at stake" problem. Here's how you can hack any proof of stake blockchain: Own 100 coins at block height 500 and stake them on chain A

Sell 100 coins at block height 510 on chain A

Create chain B by staking a new history of blocks 500-511, but remove the transaction from block 510 where you already spent your money.

So when someone's node is validating block 511... how do they know whether or not to stake on chain A or chain B? Both are equally valid according to the protocol's rules, so they can't tell the counterfeit history apart from the honest history.

Can you link some coins that have been exploited by that also what keeps KCC from being vulnerable to this type of attack as there is a lot of rising POS chains.

Marvelous - August 6, 2022, 8:44 am

(Aug 6, 2022 01:18 AM)Focus Broken Wrote: [\[CITE\]](#) Does anyone else think it's crazy that some people want to hijack \$100b in stablecoin deposits with a fork that doesn't even work in theory? How would you convince someone to switch to your fork if you can't even explain how your chain reaches consensus?

Does anyone think it's crazy that once I seen the date of the OP I knew it was Focus Broken who bumped this old thread?

Marvelous - September 3, 2022, 8:29 pm

Seen the dates of all the posts on this thread, and was surprised that it was actually Focus Broken who quoted a novel and bumped this thread..