




















The Inevitable Failure of Proof-of-Stake Blockchains and Why a New Algorithm is Needed (Op-Ed)



2054

Total views



Centralization and Blockchain Control

One of the driving factors behind cryptocurrency is the fact that it is decentralized, meaning that no individual or group controls it. Instead, it is controlled by everyone participating in the particular cryptocurrency's network. The more people in the network, the more resistant it is to different kinds of attacks.

A cryptocurrency itself has no “single point of failure,” as it would be said in the computer security world. This means that in order for someone to compromise a cryptocurrency as a whole, they would need to compromise more than one aspect of it.

For example, let's say that someone managed to break into a single Bitcoin wallet; they have not compromised the network and they have not compromised every Bitcoin wallet. They have only compromised that one Bitcoin wallet and nothing else; the Bitcoin network stays strong! That is the beauty of cryptocurrency!

Centralization in Proof-of-Work: 51% Attack

Unfortunately for Bitcoin and other Proof-of-Work (en.wikipedia.org/wiki/Proof-of-work_system) (PoW) cryptocurrencies, people figured out that if they “pool” their computing power together for the sake of mining, they can make money faster.

I am all for working together, but when it comes to mining a cryptocurrency, only one person can mine a new block at a time; if you attempt to split the reward for mining a new block among multiple miners through the blockchain, you need some proof of their work on the blockchain, which leads to blockchain bloat that nobody wants.

So, to effectively pool mining power together in a PoW system, everyone who wants to pool together needs to give control of their mining power to a central wallet, which claims the reward for all the blocks the pool mines and whose owner (hopefully) splits it among the miners based on their contribution.

Aside from the obvious trust issue involved with this kind of centralization, there is another major issue: the whole blockchain could become centralized!

Most cryptocurrencies, like Bitcoin, follow a “Longest Valid Blockchain (cointext.com/bitcoin-blockchain-the-longest-chain-wins/)” rule. This means that if two blocks are competing for the same position in the blockchain, the network will adopt whichever block has the most blocks attached after it, so long as the block is valid. Because of this, if any individual or group can get enough mining power to mine faster than the rest of the network combined (more than 50% of the total mining power), then they can modify a block and make a new blockchain based on it, which is longer than the original blockchain.

If their modified blockchain is longer than the original blockchain, then it becomes accepted by the network. If they can do this repeatedly, then they can modify the blockchain at will and have complete control over it; the blockchain becomes centralized. This is the infamous “Greater Than 50%” or “51%” attack (learn.cryptography.com/51-attack/).

Before people started pooling their mining power, this type of attack was infeasible. But now, with pools, it has become possible for pool owners to collude and break that 50% barrier. The last I checked (May 5, 2015), there are four major Bitcoin pools each controlling at least 10% of the mining power and up to 19% of the mining power. Together, they control 58% (<https://blockchain.info/pools>) of the mining power. That means that if the four individuals operating these pools decided to work together, they could rewrite the Bitcoin blockchain!



Here is why:

In Proof-of-stake, the rich get gradually richer.

If the rich are more likely to get a block, they are more likely to collect the reward for the block. Every block they get, the richer they become. The richer they become, the more likely they are to collect the reward for a block.

This keeps going on for the life to the cryptocurrency and if the cryptocurrency lives long enough, it will see 51% stake holders, or 91% stake holders, or even 99.91% stake holders. It is only a matter of time.

A Mathematical Example with NXT

Speaking of time, how long will this take? The current top stake holder of Nxt is account NXT-THLJ-CYAL-JQST-6FNS5 with a balance (nxtexplorer.com/nxt/nxt.cgi?action=30&&switch=1&sub=1) of 50,020,753.04 NXT. The current average transaction fees (which make up the block reward in its entirety) per day is 6,207.25 NXT (nxtexplorer.com/nxt/nxt.cgi?action=40). Assuming that all 1,000,000,000 NXT is being used to forge and that stake is directly proportional to the percentage of blocks forged, then this account gets about 5.002075% of the 6,207.25 NXT today. This is 310.4913 NXT. Tomorrow, this account will get even more: 5.002106% of 6,207.25 NXT. This is 310.493225 NXT. It follows this equation:

$$S_i = \frac{5,002,075,304 + 100 \sum_{i=0}^{t_{days}} P_i}{1,000,000,000}$$

(//cointelegraph.com/storage/uploads/view/551fe6d8bab3866fa06401f20ff91830.jpeg)

In this equation s_i is the current day's stake as a percentage of the total amount of coins in existence, t_{days} is the number of days, including today, that have passed, p_i is the previous days profit, and p_0 is 0 NXT. To figure out at how long it will take for s_i to exceed the acceptable limit, we simply find when t_{days} at which this happens.

How Long NXT Can Last

To simplify this I wrote a quick JavaScript program to crunch the numbers to tell me how many days NXT can last. I ran it on an online code tester from webtoolkitonline.com. I found out that it was only 370,887 days for claiming over 50% of the total stake and 465,581 days for claiming over 90% of the total stake.

If that is the case, this user should control 50% of the stake in about 1,015 years and 90% of the stake in 1,275 years. In reality, it is probably less because not everyone stakes but that gives a rough idea about how long NXT can potentially last.



(//cointelegraph.com/storage/uploads/view/9911dc710d4dc22657ef9c36ea09d966.png)

Alternative Algorithm Options

Thankfully, Nxt's PoS algorithm is very adaptable to other types proof. It works by making a “target” value for every account, which is a multiple of its balance and the number of seconds that have passed and a universal “base target” value, which applies to all accounts that I will ignore for the sake of simplicity. Every account also gets a single “hit” value, which is unique to the account but based on the signature of the previous block. When the account's “target” value exceeds its “hit” value, the account earns the right to make the next block (wiki.nxtcrypto.org/wiki/Whitepaper:Nxt#Nxt.E2.80.99s_Proof_of_Stake_Model) and claim the transaction fees it contains.

All one has to do in order to adapt this algorithm is pick a value unique to each account other than its balance! The rest of the algorithm can stay the same! Of course, there may be more unique ways to do this by creating an algorithm from scratch that may offer additional security. That is a good thing to think about for the more technically inclined, but for the time being, let's focus on some options using this algorithm as a base.

Proof of Hodl (PoH)

What about using the number of blocks an account has gone without making a transaction instead of its balance? This value may be pretty uniform across accounts at the beginning but is likely to change quite a bit over time. A coin like this would appear to make a nice long term investment and might be pricey to buy because no one would want to spend it and reset their hodl count to zero. The only real problem with this is that in order for an economy to thrive, people need to use their money to buy things. Without spending, an economy can't improve; it can't get worse either but who wants to live in a “so-so” economy? Let's consider the opposite.

Proof of Use (PoU)

What if generating new blocks was based on how many transactions someone has made and/or received over a certain number of blocks? This certainly encourages people to spend and/or buy! This may, however, be unfair to those who can't afford to make many transactions due to transaction fees and the fees would have to be high enough to prevent people from spamming the blockchain with transactions to accounts they own. The fees for using it would have to outweigh the benefit gained by spending that would change every block so fees would have to be variable, which requires some math.

Proof of Stake-Time (PoST)

Vericoin (cointelegraph.com/news/111921/vericoin-to-open-cryptobank-pay-interest-to-users-) has recently implemented a new algorithm they call Proof-of-Stake-Time or PoST. It is very similar to a variant of PoS used in Peercoin which multiplies the stake by its age. Peercoin calls this “PoS” but I would classify it under the title “PoST” because mining is based off of an account's **S**take and the **T**ime for which it has belonged to the account so really, Vericoin is just the first to use the term PoST. That being said, Vericoin's PoST has a wildly different effect on the network than Peercoin's PoST despite their similarities!

The biggest difference is that Vericoin adds a fractional multiplier to the transaction's age. The math is a little complicated, but what you need to know is that the larger portion of the entire network weight that the value of the number of coins multiplied by their age takes up, the sooner the probability to mine a block starts to drop. If not active, everyone's chance of mining a block will eventually start to drop rather than grow.

For the rich this happens sooner and for the poor this happens later but it will happen to everyone if they aren't active. The effect, as it is said in the Vericoin PoST whitepaper (www.vericoin.info/downloads/VeriCoinPoSTWhitePaper10May2015.pdf) is that you get the “active rich” against the “vested poor” as opposed to the “rich ruling” the poor or “poor attacking” the rich. This still isn't the ideal outcome but it is a much better situation than you get with regular PoS.



(//cointelegraph.com/storage/uploads/view/4157f9c9db09d3b73d330692d0d738de.png)

Proof of Minimum Aged Stake (PoMAS)

What if the right to make the next block was based only on the fact that an account has some minimum balance rather than how much balance they have? As long as an account has had some minimum balance for a period of time a multiplier for the “target” value could be chosen in a similar way the “hit” value is chosen: a way that is unpredictable but verifiable. This certainly seems fair as every account meeting those requirements has an equal chance for winning the next block.

The problem is that people with large stakes can split it among multiple accounts to improve their odds so there needs to be a way to discourage this behavior. Fees for funding an account with zero balance would have to outweigh the benefit gained by having multiple accounts and that would depend on how many accounts have balances above zero.

This, however, allows miners to manipulate the block to maximize their “target” value multiplier and “hit” value if they can still get it in fast enough. Plus, there is still the problem of finding another value that is unpredictable but verifiable. For these reasons, a second block signer who can sign the block but not make other changes to it can be used. This provides a second signature to be used that neither miner can manipulate so it is fit to be used for either the “target” value multiplier or the “hit” value, but it cannot be used for both.

So, in this version of PoMAS, a *third* block signer is necessary to provide the basis for the other value. This is kind of like adding two extra transactions to every block, even empty ones, so it could lead to block-chain bloat.


I have actually have been working to design a version of PoMAS that has no “target” value so it only requires two signatures. It is not complete and the details are beyond the scope of this article. I just wanted everyone to know that something like this might show up in the cryptocurrency world one day and it was originally my idea.

Editor's note: This article was modified to include Peercoin as the original PoS cryptocurrency.

[Mining \(/tags/mining\)](/tags/mining)
[Proof-of-Work \(/tags/proof-of-work\)](/tags/proof-of-work)
[NXT \(/tags/nxt\)](/tags/nxt)
[Vericoin \(/tags/vericoin\)](/tags/vericoin)


Did you enjoy this article? Read also:

- [Australia to Make Blockchain Voting App a Global Democratic Movement \(/news/australia-to-make-blockchain-voting-app-a-global-democratic-movement\)](#)
- [The Future of Ether: Ethereum Miners to Decide on DAO Rescue Fix \(/news/the-future-of-ether-ethereum-miners-to-decide-on-dao-rescue-fix\)](#)
- [Kim Dotcom Explains How Megaupload 2.0 Will Take Bitcoin To The Moon \(/news/kim-dotcom-explains-how-megaupload-20-will-take-bitcoin-to-the-moon\)](#)
- [Ardor - New Competitor to Ethereum Arises Amidst Reports of The DAO Attack \(/news/ardor-new-competitor-to-ethereum-arises-amidst-reports-of-the-dao-attack\)](#)
- [Blockchain Breakthrough: Peerplays Creates Open-Source Fee Sharing Module \(/news/blockchain-breakthrough-peerplays-creates-open-source-fee-sharing-module\)](#)




CoinTelegraph

17,728 likes













Like Page



Share

Be the first of your friends to like this

Follow @Cointelegraph (https://twitter.com/intent/follow?screen_name=@Cointelegraph)

