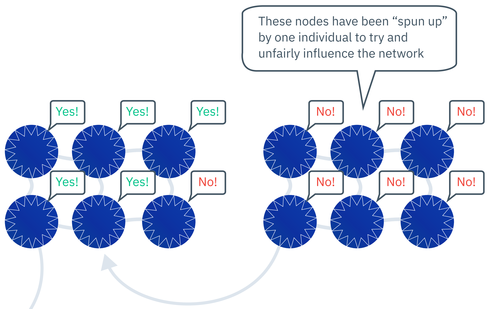
Cerberus - How Radix achieves infinite linear scalability while preserving atomic composability

Sybil Resistance Through Proof of Stake

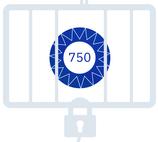
We discussed before that nodes come to consensus to commit a transaction to the ledger by reaching a majority vote on it. But what if somebody were to create lots of nodes to get lots of votes? This is known as a Sybil attack.

To prevent this, public blockchains and DLTs need a smarter way to weight the votes.

Radix uses a mechanism called “Proof of Stake” (PoS) to weight the votes of each node for Cerberus consensus.

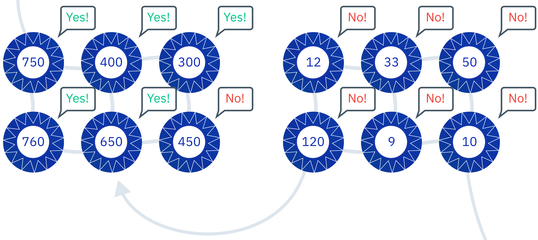


In a PoS network, if a node wishes to participate in verifying transactions, it must put down a “stake” – that is, lock up some tokens and keep them locked as long as they want to verify transactions.



Radix’s version of Proof of Stake is called Delegated Proof of Stake (DPoS) which means that token holders are incentivized to “delegate” their tokens to a node to earn a reward.

A node’s voting strength is weighted proportional to the total amount of stake locked to it.



With votes weighted by stake, if someone wanted to execute a Sybil attack, it would be much more difficult, as they would have to spend significant resource purchasing stake in the network, and all they would be doing is harming a network they now have a significant stake in!

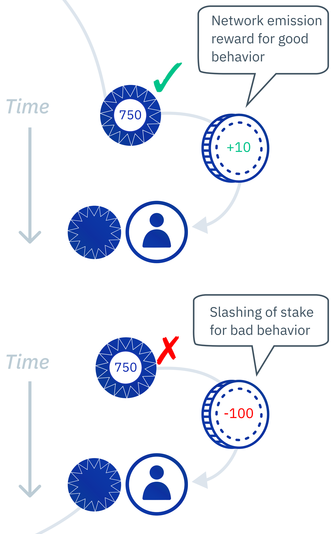
The Sybil attack depicted here would fail, as the malicious nodes don’t have enough stake.

So why stake in the first place?

If nodes behave well, and validate transactions honestly, they and the token holders who delegate stake to them earn a reward that’s proportional to the stake put in. This reward is called “network emission” and is similar to mining tokens on Bitcoin.

If a node is found to be provably malicious, then it will lose both the network emission reward, and some or all of the stake committed to it, incentivizing nodes to remain honest. Malicious behavior might be something like a “double spend”: telling some nodes one vote and other nodes a different vote to try to convince the network to process two conflicting transactions.

While the network (majority of vote weight) will try to detect and punish malicious behavior, to successfully mount such an attack, an attacker would need to control greater than 33% of the total stake, making such attacks extremely expensive.



So that’s it! Time to conclude.

The version of Cerberus described in this infographic series is scheduled to launch as part of the fully sharded Radix Xi’an release. Please visit www.radixdlt.com for details on the Radix roadmap.