

This is my attempt at creating a contract that's token supply is forcibly distributed. Distribution is good for proof of stake sidechains. This mean scaling

It basically flips proof of weak hands around in a way. The more you lose in the contract the more tokens you're rewarded. Plus some other things.

Just try to attack the "resolve token" supply.

The mechanics that run this thing are the incentive to win in a pyramid, or to use the token distribution (if you lose the pyramid) to earn trx fees on the sidechain. Or dividends from contract volume. There could be another system that benefits from the distribution. Like a dao that also runs in parallel with the sidechain. Evenly distributed voting power to vote on where funds go.

So far, from all that I have explored all attacks are extremely difficult.

The implications of the market forces and the benefit of holding resolves makes it so that ? 51% attacks require exponential time or buying power.

I have a mainnet version working. I'll launch a testnet soon though

---edit

nevermind, broken

new tests below