Nengcoin v1.7.x Hardfork Proposal

Hong Lu, Developer of Nengcoin & Cheetahcoin

4/2/2021

Emergency Hardfork Proposal to Address Timestamp Attack

Most of CPU miners on android phone or computer side probably already observed that there were tons of miner timestamp attacks on Nengcoin over past 2 days. I have been talking with commissioner constantly over this issue on the pro and cons of actions. Here we have a solution to this with Nengcoin v1.7.x hard fork proposal, with windows10/macOS wallets to be released tomorrow.

New Version: v0.8.8.0_randomSpike-v1.7.x , short hand “v1.7.x”.

As usual, the hard fork event will happen 1 week to 2 week time frame sharing with old version of wallets. After hard fork event, old version of wallet will not be able to sync to NENG blockchain.

Features to be included in this hard fork:

1. Cheetah difficulty to be raised 6x to 0.0488
2. Spike difficulty to be raised 10x to 2.4 million
3. First Second of 100% Spike diff to be changed to 50% random chance of spike or base diff

What Happened on Timestamp Attack over Past 2 Days?

Typically, USB ASIC solo miners such as futurebit moonlander2 on two rotating nodes can mine quite profitably during normal days or during reset. However due to this timestamp attack, USB ASIC did poorly even on reset with only 1 or 2 blocks only in a day.

ASIC big rigs at pool did poorly too. At shallow reset with base diff at 0.03, ASIC big rigs only mined as low as 1 block per 100 blocks because of randomSpike algo restriction plus the timestamp attack.

Over past two days, CPU miners on computer or android phone did poorly too because the timestamp attack used aggressive forward two to three minutes ahead of time to mine into cheetah diff during normal diff range.

At one point of shallow reset, we figured that this timestamp attacker mined more than 90% of blocks, out competing big ASICs, USB ASICs or CPU/mobile miners. This poses serious security risk on the NENG blockchain.

Who is Behind the Timestamp Attack?

We do not know. This could be super powered big CPU miner renting from cloud. Or maybe FPGA miner, new type of miner with similar hashrate as USB ASIC. Sefia and I discussed and hypothesized that most likely this timestamp attacker was a combo of a CPU cloud miner plus a FPGA rig.

Why Do We Need a Hard Fork to fix Timestamp Attack?

As dev we have no problems with FPGA miners if it is the case of normal proof of work mining. All miners are welcome including FPGA miners.

However, timestamp attack approach of mining is one kind of selfish mining that hurt eco-system of other miners. It imposes a 51% attack risk at low diff reset period. Economic wise, the cloud CPU timestamp attack combo with FPGA rig will cause faster block movements and increases unnecessary supply of NENG into market.

Security Improvement by Raising Cheetah Diff

One of main purpose of v1.7.x hard fork is to raise the cheetah difficulty by 6x and to improve the security and to improve the android phone mining experience. Currently we are seeing tons of NENG CPU miners, up to 200 computer or android phone miners are mining this coin either on single coin mining mode or dual coin mining mode. The average CPU mining time per block is around 10 seconds to 40 seconds per block currently. This rise of cheetah diff will

increase cost of future cloud based CPU miner attacks and improve android phone mining experience.

Although this timestamp attacker main profit driver was FPGA miner most likely in low diff range of reset, CPU cloud miner acted as decoy to force the NENG algo into shallow reset and faster block time. CPU cloud miner may have lost money on this attack, but it facilitated the FPGA mining rig to dominate in shallow reset.

Removal of Spike 100% Restriction on big ASICs or USB ASICs on 1st Second

Part of reason that USB ASICs were not able to compete with FPGA at diff = 0.03 was the huge restriction on 1st second of previous block. Currently on NENG this is imposed at spike diff of 244k difficulty. By loosening up the ASIC restriction into 50% random chance of spike or normal difficulty, USB ASICs will be able to out compete FPGA at low diff on solo mining setup.

This change is similar to that arrangement of Cheetahcoin on randomSpike algo. Cheetahcoin 1st second is same as +- 18 seconds at 50% spike diff by random chance. Now Nengcoin will change to the same setup, +- 9 seconds of previous block time, there will be 50% of spike diff chance, 1st second will have same kind of 50% random chance.

Raising Spike Difficulty by 10x

Currently Nengcoin spike difficulty is set at 244,000. We now want this to be raised to 2.4 million, about ¼ level of that litecoin/dogecoin.

Raising spike difficulty will decrease the chance of big ASICs to be hit by this spike difficulty. Although spike-triggering anti-51% mechanism works fine with CPU miners to dominate mining after spike block, it is better idea not to hit this trigger frequently.