NENG core v1.6.x Hardfork Proposal

Hong Lu, Developer of Nengcoin & Cheetahcoin

2/15/2021

Big CPU Miner Timestamp Attack on v1.5.x

Nengcoin had quite successful hard fork at year end of 2020 upgrading from v1.4.x branch to v1.5.x and cheetah diff rose 10 times from 0.000244 to 0.00244. This means that CPU miners on cheetah_cpuminer software has 10 times more difficulty to mine NENG after hardfork. This in effect is android phone mining 2.0 that improves the android phone mining experience on NENG.

However, at end of v1.4.x week and v1.5.x version from time to time, a big CPU miner timestamp attacker emerged. The big cpu miner timestamp attacker weaponized the cheetah effect in that it mined cheetah block 2-minutes-forward and 2-minutes-backward continuously to obtain more block rewards for itself while causing some negative effects on Nengcoin blockchain and eco-system.

Here we propose a Nengcoin v1.6.x hard fork upgrade solution to improve security and economy of Nengcoin and fix the big CPU miner timestamp attack issue on v1.5.x. This v1.6.x randomSpike branch code base is already on Cheetahcoin for operation for 1 month successfully with no sign of big CPU timestamp attack or any other negative effects observed.

Security Threat from Big CPU Miner Timestamp Attack

Short Term Security Threat - Negligible

The big CPU miner timestamp attacker most likely is a selfish CPU miner who just want to make over-sized profit on mining Nengcoin. We guess that most likely this big CPU timestamp attacker used cloud based renting of huge fleet of CPUs purely on cost vs profit motivations. If the renting of CPUs from cloud is cheaper than trading price of NENG at exchange, this attack will continue.

The CPU timestamp attack itself was mainly a profit driven actions so that short term security risk of 51% attack on Nengcoin is low. USB ASICs such as futurebit moonlander2 on two rotating nodes actually can profit from this attack and squeeze more profit away from this CPU attacker. Also big ASIC miners have been mining NENG continuously during the timestamp attack so that there is no domination of mining from this big CPU timestamp attack.

Long Term Security Threat – Negative Effect on ASICs

However, we think there are some negative effect on NENG security from this big CPU miner long term if this does not get fixed properly. Nengcoin security rely on Satoshi Nakamoto's longest chain rule which says that the chain with largest chainwork wins. ASIC miners contribute majority of chainwork with high difficulty blocks. Nengcoin long term security rely on retaining ASIC miners as much as possible.

The original design of Nengcoin algo splits block reward between ASIC miner vs CPU cheetah miners by 80:20 ratio. ASICs get 80% block reward in average, and CPUs (including mobile) get 20%. We want ASIC rigs to obtain majority of block rewards precisely because we need ASIC miners to contribute chainwork security in longest chain rule calculation for bitcoin style proof of work mining.

ASIC miners are blocked left and right when big CPU timestamp attacker stamp its block time ahead and backward by more than 2 minutes continuously because ASIC miners can not mine into cheetah difficulties. If majority of blocks are mined by the big CPU miner timestamp attacker with low difficulty (cheetah difficulty = 0.00244 on v1.5.x), the overall NENG long term security will be compromised and ASIC rigs will be discouraged.

Normal ASIC rigs mining NENG are good ASIC miners mining NENG day by day defending the security of the coin in exchange for block reward. This is fee for service kind of mining work provided by ASIC big rigs. Of course in this case, we do not want big CPU timestamp attack to drive out good behaving ASIC rigs.

Economic Fallout from Big CPU Miner Timestamp Attack

Big CPU miner timestamp attack also causes the blocks time to be shorter and faster with lots of shallow resets. The more blocks are coming out, the more supply are on NENG per hour, thus negative to the economics of Nengcoin.

We suspect that the big CPU miner timestamp attacker was also a big seller after winning blocks, which caused NENG price lower during the timestamp attack.

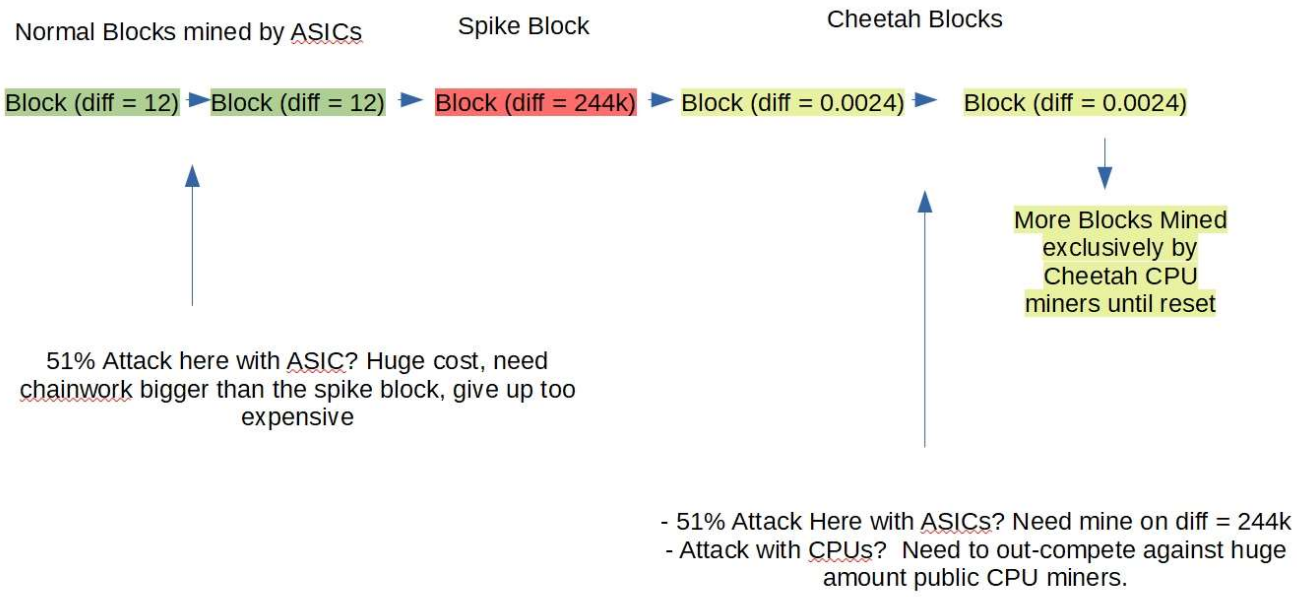
From CPU miners point of view, the big CPU miner timestamp attack was not fair to other CPU miners on computers or android phones. If a big CPU miner obtain more rewards on Cheetah CPU mining because it has more CPU powers, that would be fair. But the big CPU timestamp attacker obtained unfair advantage over other CPU miners with manipulation of timestamp back and forth. This behavior out-competed other good behaving CPU miners too in an unfair way.

What about Spike Block triggering 100% CPU Mining Afterwords?

In this proposal, we kind of defend the interest of big ASIC miners against big CPU timestamp attacker's interest. I want to play devil's advocate here. What about the randomSpike ago designed way of locking out big ASIC miners when a spike block was mined?

In that case happened in the past for NENG (see example: https://www.reddit.com/r/nengcoin/comments/kxwyy5/spike_block_mined_cpu_mining_dominating_100/), a spike block with difficulty= 244,000 was mined and the base difficulty shifted to this spike diff for ASIC or GPU miners so that only cheetah CPU miners were able to mine NENG until reset (see graph 1). Why the hell in this case spike block locking out all ASIC miners are fine here on security?

Graph 1 – Possible 51% Attack with Private Fork before or after a spike block mined



See above graph 1 on possible 51% attack before or after spike block is mined. It is clear that it is extremely difficult to plan a secret 51% attack with private fork with ASIC or with CPU rigs. I want to emphasize here that spike block case is completely different situation here. It is deceiving that virtually 100% blocks were mined by cheetah cpu miner after spike block with low diff cheetah blocks. In fact as shown in graph 1, it is quite difficult to attack the Nengcoin blockchain in this case.

A big ASIC rig with gigs of hashrate attacking NENG, mined a spike block at difficulty =244k at extremely high diff. This is a sign of danger that a 51% ASIC attacker is coming on the chain and we need to lock out all ASIC miners to protect the blockchain. In fact, in this case, 100% mined by CPU cheetah miners is quite safe because private chain fork to attack NENG is extremely costly or impossible. If the attack want to mine after the spike block, it needs to over-come the 244k diff, extremely high cost to mine for an ASIC attacker. If the attacker want to mine before the spike block, then it is competing for longest chain with chainwork for Nakamoto Consensus, the attacker need to get more chainwork than 244k diff spike block, extremely costly. If the big ASIC rig attacker want to rent a huge CPU fleet from cloud to attack NENG? Well this is getting complicated. Wallets need to be synced before doing Cheetah CPU mining, there are huge fleet of windows10, macOS, linux, chromebook and android phone dual mining Nengcoin/Cheetahcoin every day, the 51% attack need to out-compete this huge fleet? Tough and very costly to do so.

In conclusion, what we are proposing for this v1.6.x hard fork for NENG and to deny the chance for big CPU timestamp attack is completely different case on NENG blockchain security, or on economics of Nengcoin eco-system compared to spike block cases.

Details of v1.6.x Hard Fork Upgrade

1. Fix on big CPU Miner Timestamp Attack
2. Raise cheetah difficulty by 3x

The fix is quite simple on algorithm engineering level. Instead of allowing CPU miners to mine into cheetah diff for 2 minutes earlier than previous block, we simply remove that condition and impose base difficulty level of mining for 2 minutes or earlier. This fix works well so far on Cheetahcoin.

For v1.6.x hard fork, we also propose the cheetah diff to be raised 3 times to 0.0078. This was the original cheetah diff we considered on v1.5.x upgrade, but we chickened out eventually on the actual v1.5.x release. Now we have probably more than 100 Cheetah CPU miners dual mining both Nengcoin and Cheetahcoin. So now we think raising cheetah diff level again will improve Nengcoin security and allow android miners to have more reasonable reward on the hard fork.