# Cheetahcoin v1.9.x Hardfork Proposal

Hong Lu, Developer of Cheetahcoin & Nengcoin

12/12/2021

## Summary of Cheetahcoin v1.9.x Hard Fork Proposal

Here we propose that Cheetahcoin core software will have v1.9.x Hard Fork code released by end of this month and have a hard fork event happening on Cheetahcoin blockchain some time in Jan of 2022.  The expected full version is "v1.9.1.0-randomSpike-v1.9.x",  short hand v1.9.x with below features to be incorporated into the code release:

(1) Expand random spike windows from +- 18 seconds to +- 80 seconds with various degree of spike difficulty assignment probabilities from 12.5% to 75%. The v1.9.x preliminary random spike probability assignment is below counting from block time of previous block:

> +- 1 second window: 75%
> +- $2^{nd}$ second to $20^{th}$ second: 50%
> +-  $20^{th}$ second to $60^{th}$ second:  25%
> +- $60^{th}$ second to $80^{th}$ second:  12.5%

(2) Spike difficulty will drop from 100G to 20G
(3) Cheetah difficulty will rise from 12 to 36

(4) Minimum Work Bug will also be addressed in this v1.9.1 release.
https://github.com/ShorelineCrypto/nengcoin/issues/30

## Background on v1.9.x Hard Fork Release

Cheetahcoin v1.9.x hard fork release mainly follows Nengcoin v1.9.x release to address slow hack risk.

Nengcoin recently suffered its first and only 51% attack on Sep 15, 2021 on SouthXchange where 6.3 billion NENG was double spent and stolen by the hacker in a slow hack fashion. Nengcoin v1.9.1 version hard fork was released and has been operating smoothly for a while

now.

NENG last 51% attack event lasted about 1 to 2 days when the insider hacker who mined billions of NENG over past years used his/her own ASIC rig, possibly in range of 1 to 2 GH/s scrypt hashrate secretly mined a private fork with bigger amount of hashrate than public pool/solo miners of NENG.  The public pool hashrate was around 700 MH/s to 1 Gh/s then with average 1 minute per block time while the private fork was secretly mined at 30 seconds per block time lasting for 1 to 2 days hidden from public.  The insider attacker then released the private fork and orphaned the public chain and double spent this 6 billion NENG at southxchange.

The new v1.9.x release will make such slow hack on NENG very difficult or very costly because the spike difficulty serves as penalty to those ASIC miners that mine faster than the average block time desired. The faster the mining speed the more penalty on random spikes. NENG v1.9.x release has spike difficulty assigned randomly for the first 40 seconds with various random probability from 50% to 98%.

Cheetahcoin did not have that much long mining history, only started in Jan of 2021. We do not believe there exists a CHTA insider who mined hundreds of millions on CHTA on ASIC and who can pose this immediate slow hack risk on CHTA blockchain.  Never the less, this similar slow hack risk does exist too on CHTA side, hence this v1.9.x hard fork is proposed and will be implemented soon.

# Difference between SHA256 vs Scrypt

SHA256 was the first mining hashing algorithm that bitcoin uses. Mining with SHA256 requires a very high hash rate and ASIC rigs dominate SHA256 mining on bitcoin, bitcoin cash or other SHA256 altcoins.

Scrypt was adopted first in litecoin and later by other altcoins like dogecoin.  Scrypt is second most popular mining hashing algorithm that offers lighter and faster hashing calculation while it requires a bigger foot print on memory usage.  Scrypt mining currently is also dominated by ASIC rigs for litecoin or dogecoin.

Reference:
Scrypt ASIC vs. SHA-256: Explaining the Options for 2018
https://coincentral.com/scrypt-asic-vs-sha-256-explaining-the-options-for-2018/

**CHTA ASIC Mining – Digital Energy Backed by Real Cost of Energy**

I created Nengcoin in 2018 and created Cheetahcoin in Jan 2021.  Nengcoin is tech oriented coin like litecoin while Cheetahcoin is a meme coin like dogecoin.  Regardless of tech or meme, the original design intention on proof of work mining on NENG or CHTA is to maintain 80:20 ratio of mining reward split between ASIC miners vs CPU/mobile miners.

Proof of work mining offers great decentralized security with energy cost backing of mainly ASIC miners.  For CHTA or NENG,  ASIC mining are backbone of both coins and they are just like bitcoin, litecoin or dogecoin. In that sense, CHTA is a digital energy asset backed by real energy and equipment cost of ASIC mining.

CHTA CPU mining on android phones or PC are insurance of this coin in a newly designed 51% attack prevention mechanism.  Although v1.9.x hard fork may change the mining reward split between ASIC vs CPU,  it is dev team's intention to maintain that vast majority of block reward on CHTA goes to ASIC miners.

Reference on randomSpike tech:
Nengcoin Community Whitepaper:
 https://nengcoin.org/knowledgebase/whitepaper-nengcoin/

**Cheetah Effect is Much Stronger in SHA256 than Scrypt**

Cheetah effect is the main reason that CPU miners on android phone or PC can mine significant amount of block rewards in the domination of mining world by ASICs (check NENG whitepaper for tech details).

One major difference between SHA256 vs scrypt is that cheetah effect is much stronger on SHA256 side.  On 1st second spike difficulty restriction side, Nengcoin v1.9.x version imposes 98% chance for spike difficulty while we are only proposing 75% chance of spike difficulty for Cheetahcoin v1.9.x version.

Beyond 1st second random spike penalty, we use proportionally decreasing spike difficulty random chance from 75%, 50%, 25% and 12.5% when the mining speed on the block timestamp gets slower and slower counting the stamped time from the previous block.

**Spike Difficulty Lowered using Digibyte as Anchor**

Nengcoin spike difficulty at 244k has been working well for long long time.  Nengcoin also hit

multiple times of spike blocks in the past when a big ASIC hashrate attacked NENG on mining.   The chance of hitting spike blocks on NENG were rare when we only saw normal mining period with 1 Gh/s to 2 Gh/s hashrate.

Cheetahcoin has spike difficulty at 100G level for almost one year and hit spike block only one time.  We feel this level of spike difficulty is a bit too high because spike block needs to be mined when an unusually high ASIC hashrate jumped into CHTA mining.  Here we propose to decrease spike difficulty 5 times to 20G instead.

Here we can use digibyte mining hashing difficulty as reference.  Digibyte currently trades at 536 million USD market cap and its mining is on 5 hashing algorithm including both scrypt and SHA256. Digibyte's scrypt difficulty is at 101k while its SHA256 difficulty is at 1.4G.

Nengcoin's spike difficulty is 2.4 times of that digibyte's scrypt difficulty.  Our newly proposed Cheetahcoin SHA256 spike difficulty is 14 times of that digibyte SHA256 difficulty.  Using digibyte mining difficulty as reference, this 20G spike difficulty for CHTA 1.9.x hard fork should work well to increase frequency of hitting spike block as 51% attack protection mechanism, but still allowing normal ASIC mining to go smoothly without hitting spike block excessively on frequency.  Just use math proportionally on difficulty, we expect spike block will be mined 5 times per year instead of current only one time per year.

**CHTA Cheetah Difficulty Rise 3x as Scaling Solution**

Current average CPU mining time per block is about 1 minute excluding 4 minutes waiting idle time.  From past Nengcoin and Cheetahcoin hard fork experience, we know that this cheetah difficulty need to be raised from time to time as scale up solution for mobile mining.  Without doing so,  the phone mining feature will be lost when mining time decrease to 10 to 20 seconds.

With the 3x increase on cheetah difficulty, we expect CPU mining time on CHTA will slow down 3 times to 3 minutes per block.

Nengcoin already published dev roadmap for 2022 where cheetah and spike difficulty will be dynamically adjusted in stead of a fixed value. Cheetahcoin dev roadmap is going to follow Nengcoin dev roadmap closely and we are also planning to have CHTA spike and cheetah difficulty dynamically adjusted in core algorithm in 2022.