NENG core v1.5.x Hardfork Proposal, Soft Name Change

Hong Lu , Developer of NewEnglandcoin & ShorelineCrypto

11/27/2020

Soft Name Change Proposal to “Nengcoin”

Here I am leaking some community activity news of NENG recently. Community commissioner @will777 (discord) proposed to change NENG full name from NewEnglandcoin to Nengcoin. The purpose of proposal is to make NENG into next leg of path to be important cryptocurrency as store of value and payment choice.

As dev here I am fully in favor of @will777 soft name change proposal. This is major change of NENG so that community leaders (@will777 @RedRaider10 @Sefia) will provide more information and possibly seek community public feedback or votes on this issue. Here I mainly provide some comments from dev and founder point of view from my path of NENG over past two years.

When I started NewEnglandcoin (NENG) in 2018, it was started out as hobby of myself. I was and am mainly a bitcoin investor and I invested and HODL a huge percentage of my personal wealth into bitcoin in 2018. I personally invested so much money into bitcoin, I needed to educate myself deep into bitcoin code base, and I need to dig out everything behind bitcoin so that I could be sure that I did not make mistake on bitcoin, hence, I started NewEnglandcoin (NENG) in 2018. Bitcoin code base is open sourced, but bitcoin is tough to learn and test out, difficult to sync wallet. Litecoin is very much a bitcoin clone, and NENG code base was cloned after litecoin. Naturally, NENG was born.

Part of reason I picked NewEnglandcoin name was inspired by NewYorkcoin (NYC) and the fact that I live in New England. However, things changed lot since then. Currently NENG miners, investors and traders are across globe. NYC as best of regional coin has its limit, with only $1.6 million USD market cap. NENG as a scrypt coin with its unique 51% attack security mechanism and multi-rig mining method allowing profitable mining on android phone, chromebook, PC/Mac, GPUs and ASICs is very unique. In fact, NENG is currently the only coin that allow both Android phone and ASIC miners to mine on same scrypt algorithm with profit right now. A coin name should not limit the potential upside of NENG price appreciation. There is no reason why NENG should not be traded way above NYC market

cap, into tens millions of USD market cap or even on hundreds millions of USD market cap considering the fact that NENG has superior security mechanism and multi-rig mining approach on top of scrypt.

In short, this soft name change proposal is exactly the awesome path forward to unlock full potential of NENG and allow NENG investors to make a lot of money as early adopters while we still acknowledge NENG's history and heritage of starting out as "NewEnglandcoin" two years ago.

NENG core v1.5.x Hard Fork Proposal

Here we are proposing NENG v1.5.x hard fork upgrade as android mining scaling up solution with security improvement benefit. We think with this hard fork, NENG will not only has much better user experience for android phone miners, but also will get much better security against 51% attacks.

NENG android phone mining started out in summer of 2020. At beginning months of phone mining, the android phone mining result was quite good and lot of phone miners obtained equivalent mining rewards proportional to number of phone cpu cores as those CPU NENG miners did on computers.

However, the android phone mining reward deteriorated to very poor results recently. Recently we published a finding on the ROOT CAUSE on this issue here at:

why Android phone NENG cheetah mining reward Dropped Severely

https://www.reddit.com/r/NewEnglandCoin/comments/jw1z31/why_android_phone_neng_cheetah_mining_reward/

We also did some testnet testing indicating that this android phone mining scaling up issue can be fixed with a hard fork fix to increase the cheetah diff at:

Testnet 1st Try v1.5.x Android Mining Scaling Results

https://www.reddit.com/r/NewEnglandCoin/comments/k0zh6g/testnet_1st_try_v15x_android_mining_scaling/

So how this proposed v1.5.x hard fork can improve NENG security against 51% attracks? We will do a deep dive and review bitcoin PoW on this issue first.

Bitcoin – Nakamoto Consensus, Longest Chain Rule

Bitcoin whitepaper uses the concept of Nakamoto Consensus to solve the Byzantine problem of double spending issue. Nakamoto consensus centers around the proofof-work (PoW) mechanism and the “longest-chain-win” rule.

Satoshi Nakomoto first version of bitcoin software count the “longest chain” rule in a very simple way. Bitcoin blockchain may get forks naturally or even forks from attackers, but whichever the forking branch that has the longest chain with largest block number wins as “truth”. This concept of longest chain get modified later with introduction of “chainwork” considering the fact that block verses block is not same amount of work. A block with higher difficulty will cost more energy and require more work done while a block with lower difficulty needs less energy, therefore less chain work. The current bitcoin and its other clones such as litecoin, dogecoin or NENG uses this “chainwork” concept for counting the longest chain in that whichever branch with largest chainwork will win. Chainwork can be approximated with difficulty so that we can roughly say that whichever branch with largest amount of accumulated difficulties will win.

With above background of longest chain with chainwork calculation on theory, what NENG CPU miners on cheetah_cpuminer software contributes to prevent 51% attack double spending?

NENG CPU Cheetah Diff – Choking Point

NENG CPU miners mine at cheetah diff at 0.000244 or 0.0078 at v1.5.x hard fork branch. In terms of chainwork or accumulated difficulty on those CPU mined cheetah blocks, the contribution to chainwork is not that much because the difficulty is so low. So do those NENG CPU miners really contribute that much to NENG security?

Well, the answer is yes.

Cheetah effect was first discovered and introduced during the development of NENG. It has been proven to be a very huge success to prevent 51% attack which most coins in the crypto world are very prone to. The cheetah effect has been battle-tested in past two years without any 51% attack breach. The NENG blockchain auto resets to cheetah difficulty if blocks are not mined after 2 minutes. The cheetah effect can be explained by the fact that only CPU

miners with Cheetah_cpuminer software can mine on Cheetah diff. Without GPU miners, NENG is fine. Without ASIC miners NENG blockchain is fine too. Without CPU miners, NENG blockchain will be shut down.

When 51% attacker uses huge hashrate from cloud source to attack NENG, spike block will be mined and 51% security mechanism will be triggered so that only CPU miners can mine NENG because of cheetah effect. In that sense, CPU miners act as “choking point” to prevent huge ASIC hashrate from taking control of NENG network. When a spike block is mined, all 51% attackers will be in despair and watch his/her own failure with CPU miners taking all the rewards afterwards. Mining through spike diff (spike difficulty = 244,000) is extremely costly and unrealistic for 51% attackers on NENG.

What if 51% Attacker uses ASIC + CPU to attack NENG?

This is more serious threat to NENG than pure big hashrate to attack NENG. What if 51% attacker rent just a little bit more hashrate than the current NENG network hashrate and rent some CPU powers from cloud source to run CPU miners to attack NENG?

As hypothetical illustration to achieve 51% attack success, attackers need to obtain 51% of ASIC hashrate from cloud source and run several full nodes of NENG under cheetah_cpuminer software privately as “private fork”, then double spend NENG on exchange and release the fake private fork later to take over the NENG network as “longest chain”. Hula, success, double spend.

Well this is certainly a risk of 51% breach on NENG. But to achieve above 51% attack hypothetical success is not an easy task. 51% attack typically needs to be completed within 2 hours window. The time can not be too long because as soon as exchange or dev know this is happening, exchange can shut down deposit/withdraw or trading completely, or exchange can increase confirmation number to 1000 blocks on NENG deposit to cause the double spending to be extremely costly.

With this 2 hour attack window in mind, NENG cheetah diff or CPU miners again act as serious choking point for preventing 51% attacks. Sure, cheetah blocks mined by CPU miners do not contain high amount of “chainwork” because of low difficulty. But CPU mining tend to take long time. For example, in this proposed v1.5.x hard fork upgrade, we are proposing to raise cheetah diff to 0.0078. For a 3 cpu computer or 4 core android phone, it will take average 90 minutes to mine one cheetah block. 51% attacker only have 2 hours window to attack NENG for double spending, attackers can not allow 1 cheetah block to last more than 10 minutes, let alone 1 and half hours. The public NENG network has lots of CPU

miners in windows 10, linux, macOS or android phones. We project that with 30+ full nodes mining NENG on CPU, the average cheetah block mining time will only last 3 minutes per block. In order to beat the public chain for 51% attack, not only the attacker needs to rent more ASIC hashrate from cloud source, but he/she also needs to setup 30+ full nodes or equivalent 60 to 100 CPUs servers with NENG full node on cheetah_cpuminer software mining NENG privately to win the longest chainwork war. This is getting complicated and very expensive to almost not feasible.

Scaling up Cheetah Diff – White Walkers vs Night's Watch

Using TV series Game of Thrones as analogy.

51% attackers are terrible and threatening like white walkers on the picture attached here.

Night's watch are defenders on the wall against white walkers. Night's watch individual power and capability one by one could be quite weak, no match against white walkers. However, with tens, hundreds to thousands of night's watch forces allied together with forces from other kingdoms, white walkers are defeated at wall eventually.

This can be said for NENG security system with multiple rigs of Android/CPU miners allied together with GPU and ASIC miners.

At current 30 full node CPU miners count on the network, we propose v1.5.x hard fork upgrade to raise cheetah diff 32x times to have choking effect against 51% attackers on NENG.

When and if in the future NENG has explosive growth on full nodes or price appreciation, dev team find 0.0078 cheetah diff is not adequate for 51% protection, we can have v1.6.x or v1.7.x hard fork upgrade to raise cheetah diff to 0.78 or even 10 or whatever difficulty necessary to have 300 or 3000 NENG cpu miners as night's watches, a wall of choking points to protect against 51% attacks.

We foresee NENG current cheetah/spike arrangement of second layer dynamic difficulty method has no scaling problem to allow NENG to trade 10x, 100x or 1000x higher prices into multi-millions to hundreds of millions of USD market cap with hundreds to thousands of full node CPU miners acting as defenders of the wall, or wall of night's watches against menace of white walkers.