Scrypt RandomSpike - NENG core v1.3.0 Hardfork Upgrade Proposal

1. Background

NewEnglandcoin (NENG) is the only scrypt coin that allows GPU and CPU mining on the same algorithm together with ASIC miners. The goal of NENG algorithm upgrade historically was not so much of anti-ASIC goal, but rather to enable a diversified mining rigs including solo CPU Cheetah miners, solo GPU miners, solo ASIC and small mining pools so that risks of 51% attack is reduced. Double spending 51% attrack risk exist on small altcoins because it is quite easy to rent a large scrypt hashing rate from a cloud source to attack a small coin and double spend at exchange. This happened in Bitcoin Gold, NewYorkcoin etc altcoins. So far NENG has achieved history of zero incidents of 51% attack and we believe the DynDiff algo on top of scrypt helped for this achievement.

2. NENG Algorithm Change History

Below is the quick summary of NewEnglandcoin (NENG) mining algorithm.

- ASIC Mining Only - From Sep 3, 2018 to Nov. 2018, NENG mining was dominated by ASIC miners while GPU and CPU miners did not have much chance.
- ASIC/CPU Dual Mining - After v1.1.1 of implementation of dynamic difficulty adjustment in late November of 2018, ASIC miners frequently got stuck on NENG blockchain finding no blocks for hours. Since then, NewEnglandcoin(NENG) became a CPU minable coin. Initially NENG blockchain was only mined by CPU manually. After release of Cheetah_CPUminer software, CPU solo mining with Cheetah became automatic approach. During this period, GPU mining on NENG was difficult. GPU did not have much chance because GPU can not compete with ASIC on hashrate. GPU also would get stuck on NENG blockchain too, same as ASIC.
- ASIC/CPU/GPU Period – After v1.2.0 NENG core hardfork upgrade on Feb 11, 2019, GPU solo mining became profitable particularly around base difficulty reset day. Small ASIC solo miners improved profit as well while big ASIC miners or big mining pool do poorly around reset because of spike difficulty implemented in first three seconds.

3. NENG 1.2.x is subject to Miner Timestamp Attack

This was first brought up by zpool owner Jeronimo99 who now also joins NENG dev team. Jeronimo99 shared a code base and demonstrated with his own pool records that 1.2.x has weak point on its design around base difficult reset day. This weak point was not exploited that much earlier on so that effect was not obvious.

NENG miners all know that there was always some warning like "miner timestamp cheating" warning on Cheetah. But no obvious effect was known. However, on Jan 29, 2020, it was obvious that v1.2.x NENG core was attacked by a timestamp manipulating miner that left an undesirable result.

4. Explanation of Jan 29, 2020 Timestamp Attack

To understand how the miner attacked NENG blockchain with manipulating timestamp, we have to understand how NENG timestamp works. Bitcoin has this mining block timestamp rule:
https://en.bitcoin.it/wiki/Block_timestamp

NewEnglandcoin, Litecoin, or Dogecoin and many other coins never changed this bitcoin timestamp rule that much. We all have the same bitcoin rule that mainly says below:

- Bitcoin Rule 1: Miner can timestamp block with whatever time it wants. The time can be before or after current time. The mined block can also be earlier than previous block on the same chain.
- Bitcoin Rule 2: However, there is 2 hour limit that forbid a new block to be mined with 2 hours off the current time.
- Bitcoin Rule 3: A new block must be after the median time of past 11 blocks.

Bitcoin timestamp rule allows a block with time earlier than previous block. However, our implementation of v1.2.x spike difficulty within first 3 seconds also applies when the time is earlier than previous block. The timestamp attack exploited NENG spike difficulty feature in that it stamped its time 6 seconds to as much as 30 seconds ahead of current time. Honest ASIC miners were penalized by v1.2.x spike difficulty because by the time honest ASIC miner saw the time cheating block, the current time is before the mined block, therefore blocked by spike diff. The timestamp attacker could continue to mine up to 6 blocks without competition. Because of bitcoin rule 3 above, The timestamp attacker was likely to stop mining and let other miners to win some blocks. Then for a while, attack again by continuously winning another 6 blocks.

A screenshot of Jan 23 2020 Timestamp Attack from Cheetah CPUminer Message:

https://bitcointalk.org/index.php?topic=5027091.msg53725575#msg53725575

5. Why Scrypt RandomSpike is Proposed

The more important issue at stake is the risk of double spending attack on NENG blockchain is increased with this timestamp attack loophole.

We believe with this upgrade Hardfork of v1.3.0, NENG decentralization and security will be enhanced and risk of double spending attack will be reduced. The idea is not to allow one miner with timestamp manipulation to dominate mining rewards. When rewards are spread out to many solo or pool ASIC miners, solo GPU miners or Cheetah CPU solo miners, the risk of 51% attack or risk of double spending will be significantly reduced.

It is understandable that miners want to modify the timestamp for profit. But it is not very desirable for honest timestamping ASIC/GPU miners to get penalized while a timestamp cheating ASIC miner got a lot more rewards. The RandomSpike upgrade will create level playing field where timestamp cheating miner will have no significant advantage over other miners while in the meantime the decentralization and security of NENG blockchain is enhanced.

6. Technical Detail – How Scrypt RandomSpike Works

The bitcoin timestamp 3 rules will be enforced without change. The NENG specific timestamp rule will be changed.

First of all, the spike difficulty imposed on block time before the previous block is going the lifted. A block can be appended to blockchain if the blocktime is ahead of the previous block. This is will defeat the timestamp mining attack in that as soon as a miner put a cheating timestamp ahead of

current time, say 10 seconds ahead, the honest miner can mine the block attaching the current time after that.

The 3 seconds spike difficulty will be reduced to 2 seconds before and after the previous block's block time. From plus and minus 2 second to plus minus 9 seconds around the previous block's blocktime, we will impose a randomness that only 50% of chance that a block will be mined by any particular miner by imposing 50% chance of spike difficulty assignment. If the block time is 10 seconds or more before the previous block time or 10 seconds or more after the previous block time, no spike difficulty will be imposed, only regular base difficulty applies.

The way we will do it is that we can use block timestamp plus blockchain number to create a random chance, 50% of chance that a block will be accepted or rejected. We think using timestamp+ block number as seed will create 50% randomness that miner would not control.

The idea is that a timestamp miner can attack NENG, but as soon as a forward or backward timestamp block is mined, an honest miner can jump in and will mine at similar win rate. Plus and minus 9 seconds is about 18 seconds window that is quite wide. If a timestamp attacking miner place its timestamp within this 18 seconds window, it will face 50% rejection and benefit to other honest timestamp miners for next win. If an attack place a timestamp ahead or behind by more than 9 seconds, it can win a block, but the next blocks are likely to be shared with other miners. In other word, all timestamp miner can do is that it can mine a few more blocks, but not mine significantly more than other miners with similar hashrate. By reducing the win rate for timestamp cheating miner, mining decentralization is achieved.