Cheetahcoin v1.8.x Hardfork Proposal

Hong Lu, Developer of Cheetahcoin

7/3/2021

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 Cheetahcoin over past couple of weeks. We were puzzled by this timestamp attack two weeks ago. On 6/30/2021, we think we observed the in and out of the attacks and here we propose a solution to this issue.

New Version: v0.8.9.0_randomSpike-v1.8.x , short hand “v1.8.x”.

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

Features to be included in this hard fork:

1. Cheetah difficulty to be raised 3x to 12
2. Update the seed IP addresses in the wallet to improve syncing speed.

What Happened on Timestamp Attack over Past Weeks?

This CPU timestamp attack awefully now look like the one before the NENG hardfork, on NENG v1.6.x branch when the CPU attack was decoy, the main profit was on regular low diff from FPGA (or another big CPU miner). The sequence of attack also look similar. Lot of cheetah diff attack at high difficulty period, mainly for decoy, use CPU to get shallow reset. Then in the shallow reset, FPGA jumped in for the profit, and CPU device throwing 1 hour

timestamp mining cheating time (1 hour ahead) trying to stop for 1 hour to maintain low diff. So it was two device combo attack.

During shallow reset period when diff was below 100, we noticed this decoy CPU miner was still doing 1 hour ahead operation, trying hard to control the CHTA blockchain. When the chain was in control, the second device FPGA (or another big CPU cloud miner) would have then mined on normal difficulty with 1 hour ahead. It may have sophisticated software to maximize profit. It put 7 continuous blocks with 1 hour ahead. Once 7 blocks with 1 hour ahead block is in, no-one can mine, everyone have to wait. The attacker has to wait too for 1 hour due to bitcoin Median Past Time (MPT) Rule and 2 hour rule:

https://blog.bitmex.com/bitcoins-block-timestamp-protection-rules/

So CPU timestamp purpose on reset low diff period is to stop the chain moving too fast, make it one hour no blocks, then suddenly a lot of blocks by FPGA (or a big CPU on cloud). Because ASIC USB still gets blocks in this scheme, not all goes to the attacker. Big ASIC rigs are stopped, the attacker gets a lot profit on FPGA side. Still could be on profit.

The purpose of stopping the blockchain for 1 hour is to make the diff at low. Because the main profit is on FPGA or CPU on cloud, low diff is needed for more profit.

When the FPGA (or big CPU cloud miner) achieved this manipulation, it can shut down mining for saving cost, then wait for 1 hour, and then start again to attack.

It is still a more or less two device attack. The first attack is to put into shallow reset, in shallow reset, it uses this 1 hour pause approach to control CHTA chain at low difficulty. It throw some bones to other USB ASIC miners at shallow reset because it can not control 100% of mining reward. FPGA or cloud CPU mining, two device combo attack.

We believe the timestamp attack that we saw over past several weeks imposes security risk on Cheetahcoin blockchain, therefore, we propose a cheetah diff rise of 12x to address this issue. The security risk mainly was on the low diff 1-hour-pause-and-attack period although the high diff decoy attack period was not of any real security risk.

Timestamp Attack Effect on USB ASICs

Overall, USB ASIC solo miners are least affected by this timestamp attack. USB ASIC solo miners continues to obtain profit during normal or reset period. Each resets USB ASIC solo

miners obtained less profit due to timestamp attack, however, timestamp attacks tend to get more reset frequency, therefore benefiting profitability of USB ASIC solo miners like gekkoscience newpac devices.

We noticed that during low diff shallow reset period when diff < 100, the USB ASIC solo miners were not effective against the two device timestamp attack.

Timestamp Attack Effect on big ASICs

ASIC big rigs at pool did poorly during shallow reset. Usually a reset is great boom for both USB ASIC like gekkoscience newpac solo miners or big ASIC solo/pool miners as the pool big ASIC usually get 10% or more of blocks reward during this period. In the past timestamp period, we noticed that pool ASIC miners almost got no blocks when the diff was below 1k.

Timestamp Attack Effect on CPU miners

Over past two days, CPU miners on computer or android phone did poorly too because the timestamp attack used aggressive forward 1 hour method to obtain cheetah blocks during high diff period.

CPU miners on computers or android phones are powerless against this kind of aggressive two device timestamp attackers.

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

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

However, timestamp attack approach of mining is one kind of selfish mining that hurt eco-system of Cheetahcoin. 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 CHTA into market. It decrease profit of big ASIC rigs during reset period.

Security Improvement by Raising Cheetah Diff

Raising cheetah diff works on this issue on a simple math. Say if $1000 USD cost for cloud big CPU attacker on timestamp cheating, how about if we raise cheetah diff by 4x times? $1000 USD cost becomes $4000 USD cost for attack, that surely will stop the attack from trying.

But if the trading price of CHTA goes up 4 times, $4000 USD might be profitable again for the same attack to retry. What about raising cheetah diff by 16x? The cost becomes $16,000 USD for the same cloud CPU attacker doing same thing.

Of course, factoring in the security need of Cheetahcoin and interest all miners (big ASIC/USB ASIC/CPU/Andorid), we here propose this v1.8.x hard fork upgrade to improve all miners experience in fair treatment while we maintain our coin security free from 51% attack breach.

Impact of Cheetah Diff Rise on CPU/Android and USB ASIC Miners

CPU/androids mining time will increase 3x . Say mining for 1 minutes becomes 3 minutes mining time. More power usage on phones. On reward, probably similar as before as they are shared across different miners. Less timestamp attack, more reward and better chain security too.

.

USB Miners, reset will go to 12 diff only, so yes, the reset cycle is shorter. But we have to factor in the timestamp attack effect. With this timestamp attack from CPU/FPGA, USB ASIC was not really in great shape. We observed majority of block rewards now still went to the attacker on the two devices when the shallow reset diff is below 100.