Thor´s Hammer Protection

SnowGem mPoW 51% Attack Solution

Documentation

29th January 2019

Preliminary

There have been a number of recent *51% double spend attacks* in the crypto space during the past months. This has created a necessity to create a solution to help prevent these types of attacks on SnowGem. We will implement the Masternode Proof-of-Work (mPoW) system that uses the existing SnowGem Masternodes to secure the blockchain and help prevent *51% attacks* from being successful. We are calling this system Thor's Hammer as a symbol of power and protection. This is an important step in helping to secure the SnowGem blockchain as there is an increasing amount of *hash power available for rent*.

Basic Principle

SnowGem Masternodes are enabled to verify block hashes before accepting a reorganization on the chain. This is achieved by comparing a previous block hash that should be the same in both chains. If the hash does not match the Masternode will reject the new chain as it is not the consensus chain.

Any of the SnowGem Ecosystem services such as *Exchanges*, *Pools* and *Shared Masternodes* can reduce the possibility of being targeted by a *51% attack* by enabling the Masternode protection function of their wallets. This sets the wallets to only communicate with the Masternodes and other wallets that have the Masternode protection function enabled. Any wallet that has the function enabled will also verify block hashes before it accepts a reorganized chain. It is recommended that all services that accept or trade with SnowGem allow a minimum of 10 confirmations before finalizing deposits.

When the wallets are running with Masternode protection, they will allow a reorganization of only 10 blocks, an attacker must finish their work in that period, however their deposit is not finished because of exchange confirmations, they will not succeed.

*even with 99% Masternodes and 51% mining power, network is still secured

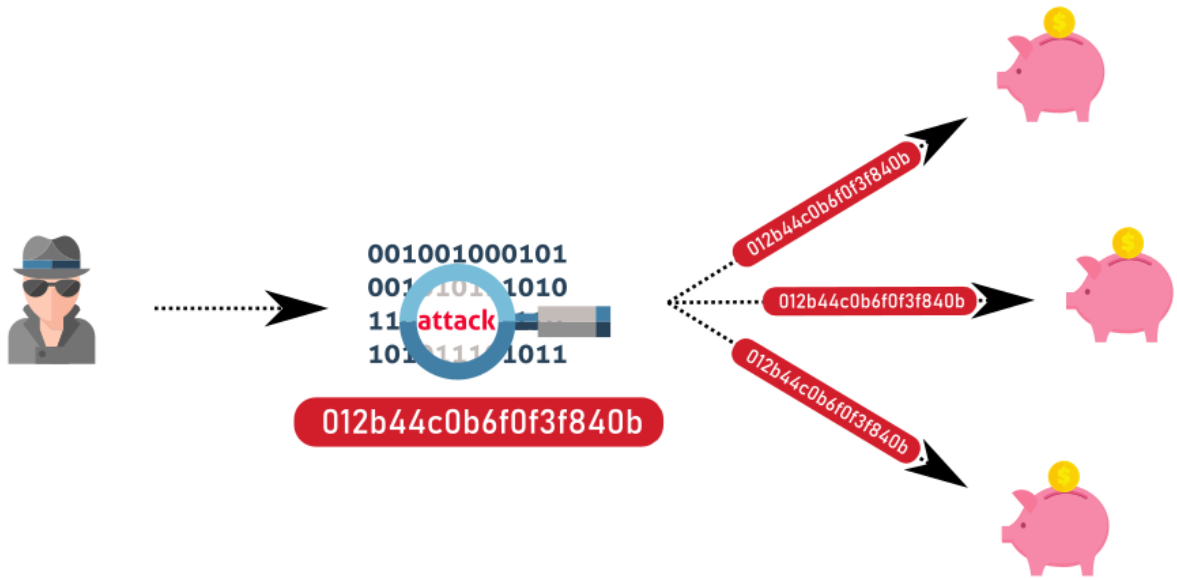
How does it work?

51% double spending attack theory

Before we can go further, you need to understand how a *51% double spending attack* works and how it can be achieved.

When an attacker wants to create a *51% double spend attack* they must complete a number of steps for this to be successful. The attacker will prepare a private mining pool with enough hash power to keep finding blocks at the same rate as the network. This requires approximately 51% of the current hash power of the active network.

The attacker will then send the coins that they wish to perform the double spend attack with. These coins are normally sent to an exchange so they can be traded for another coin or currency and withdrawn from the exchange.



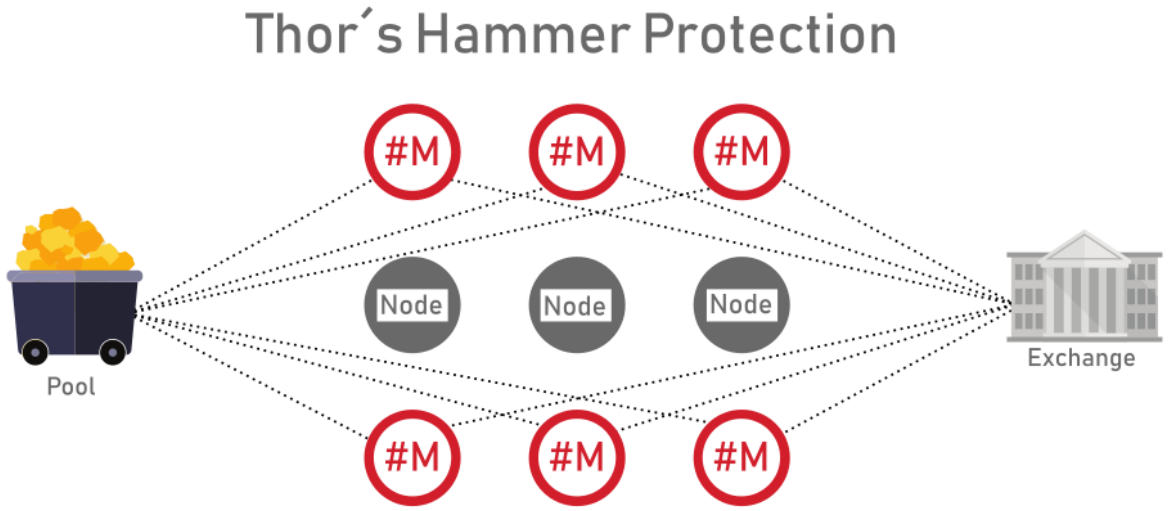
At the same time as this transaction the private pool will still mine but the transaction that was sent to the exchange was not included in private chain.

Once this is completed the private chain that is being mined, without the attack transaction that was sent to the exchange in the chain is broadcasted to the main network. The main network will detect the new chain, which will be timed so that it has more blocks then the normal chain. This action causes a *reorganization* of the blockchain. Because blockchains are configured to accept the longest chain, it causes all of the other wallets, pools and exchanges to switch to the attack chain. The result of this is that according to the new chain the exchange never received the coins that have been sold, and they are again back in the attacker's wallet.

This would be considered to be a *successful attack*; the attacker would have the original coins that were sent to the exchange as well as the additional coins that were withdrawn from the exchange.

Thor's Hammer

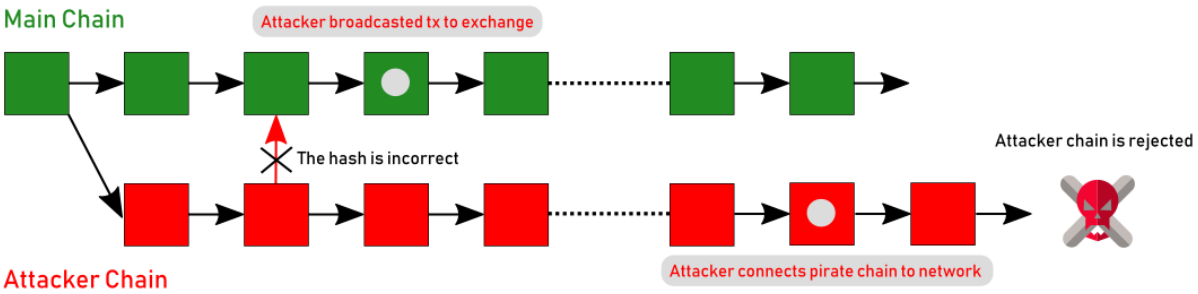
Thor's Hammer will task the growing SnowGem Masternode network with protecting and securing the blockchain. This will be achieved by enabling Masternode protection for exchanges and pools. This is done by allowing exchanges and pools to communicate with the Masternode network directly and also protect them from reorganization process.



All of the Masternodes will check a detected reorganization caused by an attempted 51% attack with their own local blockchain.

When the Masternode detects the longer chain, instead of starting the reorganization process it will verify block hashes from its own chain to the new chain. If the block hash does not match the existing chain the Masternode will reject the new chain and maintain the original chain. This action will break the attempt to perform the double spend. The attackers chain will be rejected by the Masternode network and protected nodes, the exchange will not be affected.

Blockchain diagram



Technical Details

- Addition of new configuration flag `*masternodeprotection*` this value can be either;
  - 0 (off)
  - 1 (on)
- Setting the value to 1 will enable the Masternode protection system for the wallet.
- Addition of new configuration flag `*masternodeconnections*` this value can be either;
  - 0 (off)
  - 1 (on)
- Setting the value to 1 will limit the wallet peer connections to active Masternodes.
- Masternodes will continue to connect to all peers, both Masternodes and normal wallets.
- Masternodes and wallets with `*masternodeprotection=1*` will, in the event of a reorganization detection on the network compare the new block height - 10 block hash with the corresponding block height of the existing chain. If the hash does not match for that block, the wallet will reject the reorganization as invalid and continue on the existing chain.

Attack test on secured network

We successfully tested 51% attack on secured network (testnet) as you can see it on this video: https://www.youtube.com/watch?v=sdqw2rv8pzE

The Thor's Hammer was able to detect the invalid chain and blocked the reorganization that would have completed the *51% attack*. The attackers private chain was rejected, and forced a reorganization to the original chain for attackers pool.

Conclusion

The SnowGem team is working hard to provide a more secure and safe network and future for the SnowGem Ecosystems. With the release of Thor's Hammer we believe that this is a major security improvement to the existing network and will significantly reduce the possibility of a successful *51% attack* on the SnowGem network. The use of the Masternodes to actively monitor and protect the SnowGem blockchain as a network service will further emphasise the importance of the the Masternodes as an integral part to the continued successes and security of the SnowGem project.