



PROFIT HUNTERS COIN WHITE PAPER 1.0

A digital currency for a decentralized affiliate marketing platform

www.ProfitHuntersCoin.com

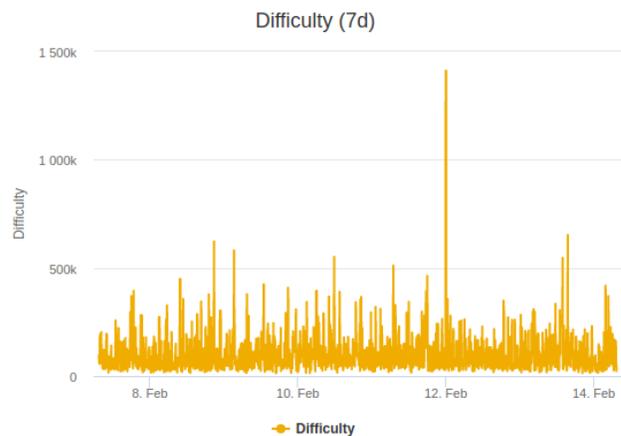
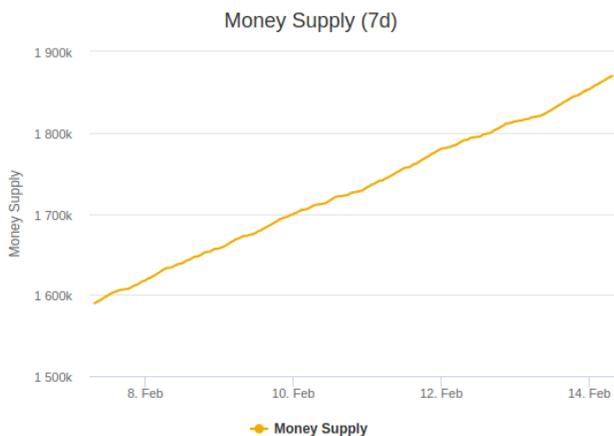
Last edited: April 25, 2018

"I think Bitcoin has been one of the most significant projects empowering people of all wealth classes, nationalities, and religions to cooperate." - Justin Percy, Founder of PHC



PHC is a Proof of Work, Proof of Stake & Masternode based crypto-currency to be used for affiliate opportunities and online marketing. It's a coin intended to be adopted by beginner and advanced crypto-currency users, it will be promoted through affiliate marketing in a peer to peer social network platform. Third party affiliate marketing services will be invited to join the social network, integrating their business solutions directly - offering incentives, rewards and commissions paid in PHC. Direct marketing campaigns on the platform will revolutionize how new opportunities are promoted and discovered, giving users the ability to communicate directly with each other, offering real-time permanent reviews that become stored on a custom side chain. Decentralized solutions can easily be implemented with PHC using existing technology available for Bitcoin.

Dynamic Block Reward 3.0:



$$\text{PoW Block Value} = \text{SubsidyMax} - (\text{NetworkHashPS} / \text{Difficulty})$$

The block reward is calculated based on the last block's difficulty and current network hash-rate. If the network hash-rate jumps up a lot during low difficulty then it will result in a low block value. Some pools and miners are configured that when the difficulty goes up they usually switch over to another coin - leaving a very difficult block for low hash-rate to solve. PHC tries to automatically discourage this behaviour. When the difficulty is high and hash-rate is low - those are the most profitable blocks to solve! Pool jumpers are merely scratching the

surface of their potential earnings. The block rewards for each block are not static, and fluctuated over time as they *adjust dynamically with live-network conditions*.

If you would like to start mining with the least amount of power as possible for the most profit: you can join a pool when the network difficulty is high and the network hashrate is low, this will cause the block reward to increase in value!

If you decide to start mining with a lot of hash-power during a time of low difficulty: the block reward will decrease in value, making it very difficult to earn a profit for your extreme efforts. Not to mention, by doing so: You drive the difficulty up significantly, and if that triggers a pool's auto-coin switching script to move onto another alt-coin. Then your mining efforts, in terms of increased revenue... Will actually go to the workers who remain on the network consistently.

Reward adjustments based on network hash-rate, previous block difficulty simulating precious resource mining. If the difficulty rate is low; using excessive work to produce low value blocks does not yield large return rates.

When the ratio of difficulty adjusts and the network hash-rate remains constant or declines: The reward per block will reach the maximum level, mining becomes very profitable at this time. Dynamic Block Reward 3.0 algorithm is intended to discourage greater than 51% attacks, or malicious miners. It will also act as an automatic inflation adjustment based on live network conditions – avoiding malicious miners that “hyper-inflate” coins and then quick sell.

Minimum PoW Reward:1 PHC

Block #1 Up to 50000	[Max PoW: 100 PHC]	[Max PoS: 1000% APR]
Block #50001 Up to 100000	[Max PoW: 50 PHC]	[Max PoS: 500% APR]
Block #100001 Up to 150000	[Max PoW: 25 PHC]	[Max PoS: 250% APR]
Block #150000 Up to 200000	[Max PoW: 12.5 PHC]	[Max PoS: 125% APR]
Block #200001 Up to 250000	[Max PoW: 6.25 PHC]	[Max PoS: 250% APR]
Block #250001+	[Max PoW: 3.125 PHC]	[Max PoS: 250% APR]

A few examples (Max 50 PHC - Block #50001 Up to 100000):

Example 1	Example 2	Example 3	Example 4
<u>Hash-rate:</u> 52766	<u>Hash-rate:</u> 52766	<u>Hash-rate:</u> 527660	<u>Hash-rate:</u> 5276600
<u>Difficulty:</u> 92953	<u>Difficulty:</u> 929530	<u>Difficulty:</u> 92953	<u>Difficulty:</u> 92953
<u>Block value:</u> 49.43	<u>Block value:</u> 49.94	<u>Block value:</u> 44.32	<u>Block value:</u> 1.00

Difficulty is adjusted every 2 blocks, and if miners drop from the network during high difficulty (like they usually do) then the block reward becomes near the maximum. If the high hash-rate stays steady for a long period of time - the difficulty adjusts and the reward recovers too.

Security Aspects of the Dynamic Block Rewards:

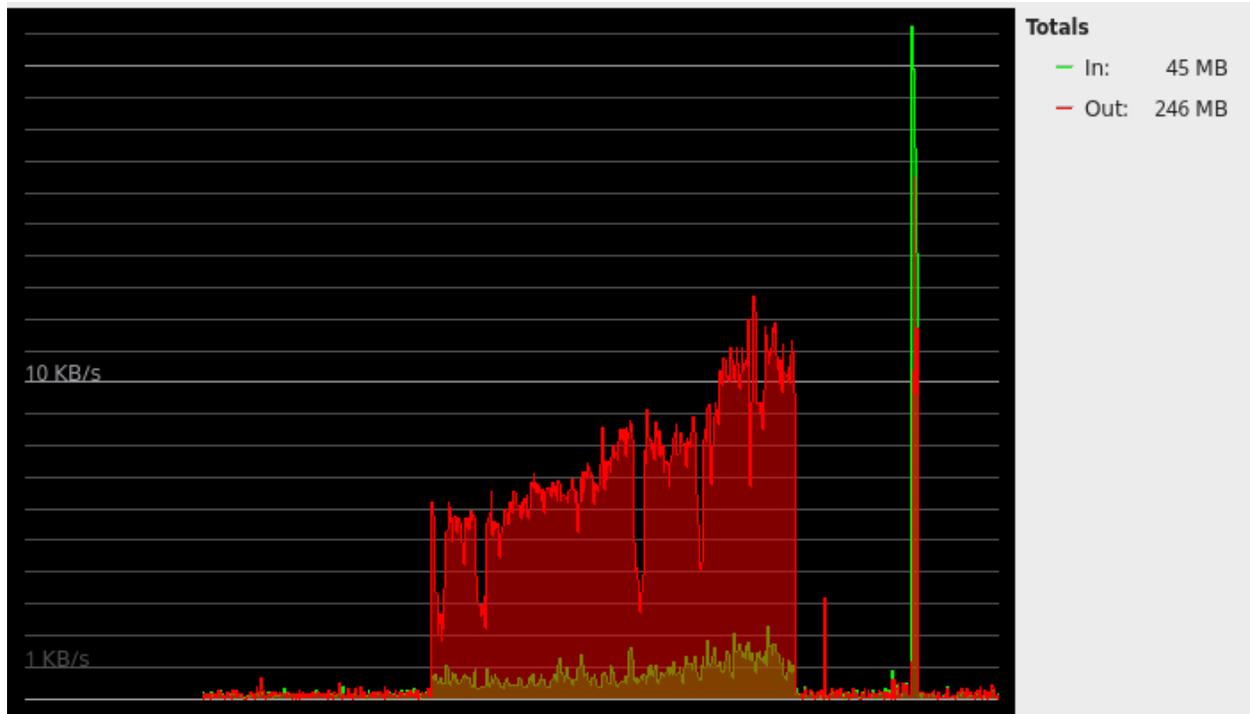
Acts as a secondary hashing algorithm, by chaining blocks together based on time-sensitive network dependent variables. It's very difficult to attempt to fork the chain with orphan blocks maliciously generated, because the block value will depend on the previous difficulty and current network hash-rate and won't pass the ConnectBlock() check from other peers.

```
Postponing 89 reconnects
REORGANIZE
REORGANIZE: Disconnect 818 blocks: 3b22b819b073e50f52bb6743e7a8858634105018af268c649be4f06b53f5faf4,,a3df52b7197
REORGANIZE: Connect 60 blocks: 3b22b819b073e50f52bb6743e7a8858634105018af268c649be4f06b53f5faf4,,11e670e63bb9d99
connect() to [2001:0:9d38:6abd:1837:cb1:8cb2:416f]:20060 failed: 101
ERROR: ConnectBlock() : coinbase reward exceeded (actual=5500000000 vs calculated=4800000000)
InvalidChainFound: invalid block=41b1f47e835cc00b0ed0a5b24c954af48f3e72f5b187316fef8eb2bcc1ff7be6 height=38189
InvalidChainFound: current best=a3df52b71973b85095d71dc1948430daa5e9f21ab8d894bf317fcc9ab6857102 height=38858
ERROR: SetBestChain() : Reorganize failed
ERROR: AcceptBlock() : AddToBlockIndex failed
ERROR: ProcessBlock() : AcceptBlock FAILED
ProcessBlock: ORPHAN BLOCK 243, prev=0e441ecc3618efb9aa1c4bf83d15d18a2d474c2075d620fa63c414b1ee2a82ca
```

Technically the "lost" block-reward is not burned because it was never created, but in essence; It could be considered similar to "burning" it, instantly. If you're trying to make a long-term profit it won't affect you much as a miner or PoS/MN. If you're a pump and dump group renting or using mining equipment for an attack, you might reconsider "giving up quickly" if the price doesn't automatically adjust based on the increase in difficulty on the network. Especially if you can't inject "forked-blocks" with >51% hashpower.

Bitcoin Firewall 1.2.2.1

World's first Bitcoin Core 8 implementation of connections firewall & intelligent attack detection



As shown in the picture above. The attack appears to be very advanced. Multiple peers are used. 1 or more peers forcefully broadcast the beginning of the forked chain (mined off-network). Mining pools that accept the blocks struggle to calculate the chain best height based on the new orphans, the consensus algorithm attempts to merge these questionable blocks. If the mining pool achieves greater than 51% of the network hash-power they can prioritize the forked chain to be confirmed faster than blocks of the same time frame. If this pool solves and sends newly generated blocks; Built on-top of the forked chain quicker than the existing network, the consensus algorithm forces all peers to view the forked chain as valid! The firewall prevents this because it simply "cuts off" a section of the forked chain to ensure new generated blocks from the attacking/affected pool (ahead of the existing network) are ORHANS because the chain is BROKEN.

Bitcoin Firewall uses a very unique method for detecting potential hard-fork chain-attacks coupled with specific block chain DDoS flooding. All connected nodes/peers are examined by the amount of data they're sending or receiving from a peer with the firewall enabled. If bandwidth usage is greater than the limits set, the connecting node is further examined to verify their blockchain start & sync height. The average among all peers connected is considered safe. Range based blockchain checkpoints that use averages of live blockchain sizes further enhance security by limiting potential attacks known as >51% of distributed hashing power (double-spend, Sybil attack).

Coupled with other advanced detection rules, this has proven quite successful in mitigating chain fork attacks or network flooding. Once a potential attack is detected the connected node/peer is forcefully terminated and added to a session blacklist and or banned.

Specifications:

- **Algorithm:** Scrypt (Litecoin)
- **Genesis Date:** GMT: Monday, January 1, 2018 10:00:00 PM
- **Max Supply:** 100,000,000 PHC (1 hundred-million)
- **Premine:** 0 PHC
- **ICO:** no
- **Air Drop:** 0
- **Block Spacing:** 60 Seconds (1 minute)
- **Diff Retarget:** 2 Blocks
- **Maturity:** 101 Blocks
- **Stake Minimum Age:** 1 Hour
- **Master-node Collateral:** 10,000 PHC
- **Stake Combine Threshold:** 1000 PHC
- **Reward Distribution:** 75% to Master-nodes while 25% to Staking wallets.
- **30 MegaByte** Maximum Block Size (30X Bitcoin Core)

Staking:

Leaving your wallet online with an available balance of 1000 or more PHC will earn you random interest payments on transactions. Your wallet confirms new transaction blocks using the Proof of Stake algorithm. The amount you earn will be proportional to the total amount of coins available and their age as well as the total value of all inputs for the block solved.

Master-nodes are another way to stake and assist the network security and dependability. These require 10000 PHC for stake collateral and are randomly chosen among all master-nodes for up to 75% of network stake commissions. They offer superior security with cold and hot wallet modes.

The most cost effective solution is to order a VPS (Virtual Private Server) and setup a remote controller wallet with your collateral coins. This allows network traffic to connect to your slave wallet without opening up vulnerabilities to compromise your controller wallet (collateral coins)

Future Plans:

- Find and Fix bugs in the core 8 code, masternode, proof of stake and Bitcoin Firewall.
- Marketing to more exchanges, forums, and social networks
- Integrating PoW/PoS/Masternode source code into Bitcoin Core 10
- Creating a social network platform for beginner to advanced crypto-currency users and affiliates.
- Partnership and affiliate marketing solutions engineered for financial technology companies.
- Suggestions are welcome!

No timelines have been set for future developments, this project is volunteer based and progress will advance as new developers join and development master-node funding is established.