

Bitcoin Interest Equinox Update

By Aaron Mathis



INTRODUCTION

Bitcoin Interest has been around since January 20th, 2018 and we have learned so much in this short amount of time. One of the things we have treasured most is our community response to the project. We are devoted to always bettering ourselves and listening to constructive opinions. I hope you will enjoy this update and the exciting things we have coming.

What is Equinox?

Equinox, also known as “Version 2”, is the name for the first major update to the Bitcoin Interest Core Wallet and platform. Below I will address the changes that will be happening and what it means for you as a coin holder.

Why are you performing an update?

We believe that time has no relation to performance and we feel improving our product is the best approach to better serving our community. We have two major updates that will result in a hard fork once the ProgPoW research has been completed. A block height will be selected and that will define the date of the hard fork.

1. Changing from Equihash to ProgPoW

We are changing the algorithm of Bitcoin Interest to combat the new Equihash ASICs. Though nothing is truly ASIC resistance, we feel this algorithm offers a perfect long-term solution to secure our chain for years to come and to always give GPU's a chance against ASICs.

2. Interest is getting better

Segregated pools are here! User's will now be separated into different pools depending on the amount of BCI coins they are participating with. This new setup stops whales from dominating the interest pool and promotes a fair opportunity for everyone. We are also adding new staking schedules and a brand-new feature called 'Staking insurance'.

3. Halving is a thing of the past

The Bitcoin Interest mining reward for solving a block will no longer be halved from 12.5 BCI coins down to 6.25 coins in the next two years. Users can expect mining rewards to stay the same for the next 5.5 years! Near the end of this time we will implement one of the many solutions to keep mining profitable and alive, or should a new technology emerge we will explore any new options our community may ask of us.

4. Masternodes (Possibly V3)

Masternodes are on our list of things to add to help with transaction and create a more secure network.

5. Proof of Ownership

Exactly what it says. Addresses will now be validated before staking, however, this process will be free and only requires the signing of messages.

6. Smaller Blockchain

The current size of the blockchain is around 180GB and this makes it difficult for the average user to use the Bitcoin Interest wallet. To make it easier on these users, we will be resetting the chain back to block 1. Note: Users can still use their BTC private key to claim the BTC 1:1 BCI fork coins.

Programmable PoW (ProgPoW)

Information taken from: <https://github.com/ifdefelse/ProgPOW>

ProgPoW is a proof-of-work algorithm designed to close the efficiency gap available to specialized ASICs. It utilizes almost all parts of commodity hardware (GPUs), and comes pre-tuned for the most common hardware utilized in the Ethereum network.

Ever since the first bitcoin mining ASIC was released, many new Proof of Work algorithms have been created with the intention of being “ASIC-resistant”. The goal of “ASIC-resistance” is to resist the centralization of PoW mining power such that these coins couldn’t be so easily manipulated by a few players.

This document presents an overview of the algorithm and examines what it means to be “ASIC-resistant.” Next, we compare existing PoW designs by analyzing how each algorithm executes in hardware. Finally, we present the detailed implementation by walking through the code.

The design goal of ProgPoW is to have the algorithm’s requirements match what is available on commodity GPUs: If the algorithm were to be implemented on a custom ASIC there should be little opportunity for efficiency gains compared to a commodity GPU.

The main elements of the algorithm are:

- Changes keccak_f1600 (with 64-bit words) to keccak_f800 (with 32-bit words) to reduce impact on total power
- Increases mix state.
- Adds a random sequence of math in the main loop.
- Adds reads from a small, low-latency cache that supports random addresses.
- Increases the DRAM read from 128 bytes to 256 bytes.

While a custom ASIC to implement this algorithm is still possible, the efficiency gains available are minimal. The majority of of a commodity GPU is required to support the above elements. The only optimizations available are: *Remove the graphics pipeline (displays, geometry engines, texturing, etc) *Remove floating point math

These would result in minimal, roughly 1.1-1.2x, efficiency gains. This is much less than the 2x for Ethash or 50x for Cryptonight.

Why did we choose ProgPoW?

ProgPoW offers some great benefits and helps combat ASICs. The OhGodACompany has been in close contact with us and we feel this will be a great partnership with them alongside us.

Have you started implementing this algo yet?

As of now we are in the research phase and determining the best way to approach the change. This will be a complex task and will require a good amount of though long before we begin programming.

Interest in Equinox

We have learned so much from this first version of our interest platform and have heard a great deal of feedback from the community on ways to improve an already loved concept. Below we will outline the changes coming and what it means for you.

Segregated Pools

What does segregated pools mean? Well this is our concept to help address the issue of whales dominating the interest pools. One person should not be able to earn 50% of the interest pool at a given time. This is where segregated pools come in. These pools will be applied to the monthly and weekly staking process.

There will be three interest pools now and which pool you will be in will be based on how much you can stake.

The pools will be:

- Bronze Pool
- Silver Pool
- Gold Pool

These three pools will now allow for users to have a more equal and fair chance of gaining interest without having to worry about someone coming in to dominate over their coins.

You will be in a pool based off your staked amounts.

Bronze pool is anything from 0-2000 BCI, Silver pool will be 2001-8000 BCI, and the Gold pool will be anything 8001 BCI and up. These pools are designed to maximize reward potential and actually benefits those wanting to stake 1 BCI or 10,000 BCI. The pools will not punish, but actually reward you as you will be competing more against people closer to your stake amounts, thus granting a great chance at a higher interest rate.

In the current system, if you staked 1 BCI in the monthly pool, you'd get somewhere around 0.02 BCI for the entire month. Whereas in the new pool structure you'd have a greater potential of earning around 0.1 BCI, which is a 10% reward instead of 2%!

Two New Staking Periods

We will be adding two new staking periods for even more earning potential! We will be offering the following new periods:

- Quarterly
- Yearly

This will now allow you to stake your coins for even longer and increase your earning potential. These periods will also have no set dates like monthly and weekly. You will be able to stake at any time for these cycles and get guaranteed interest rates for them. Rates will be set on a monthly basis and once you stake it will be locked in for you and guaranteed.

Staking Insurance

We understand that since coins are in your possession and not ours it is easy to make a mistake and move them out of your wallet. We know this has caused a lot of users issues, especially for monthly stakers, so we are now going to offer staking insurance. Note: only round insurance won't be offered for is weekly.

What does this mean?

If you elect to purchase staking insurance, you will be given an extra 48 hours to fix whatever issue with your staking account there may be and NOT lose eligibility for that round as long as the round doesn't end before you fix it. You will be notified via email to correct this once an error has been detected by our system.

What will insurance cost?

Insurance cost will be based on the pool you are in and will be a flat cost for each pool at a different price point. These price points have not been finalized, but they will be rather cheap for the protection they offer, especially for those staking quarterly and yearly and don't want to risk losing all their hard work if they accidentally send coins elsewhere.

Are miners going to get taxed more since interest rewards are higher?

Simple answer is no. We are still going to leverage our split block reward system, where we don't touch the original 12.5, or we keep it at the very least above 12.4. This may require a small increase in total supply, but nothing that will affect the overall stability of the coin.

No more halving of block rewards

We are really happy with where our block reward is at and feel a halving of the reward and interest would cause an overall general disinterest in our coin. Because of this we have decided not to follow the bitcoin halving schedule and will be removing that function altogether.

What does this mean for coins left to be mined?

This means at current rates we have about 5.5 years of really good mining and rewards left. We feel this is more than adequate as this industry is evolving and PoW is changing so much every year that by the time those 5.5 years are up we are confident to say our coin will have evolved and there will be no issues regarding this.

Some obvious solutions though to this concern could be these:

- Increase Max Supply
- Move to all staking (PoS)
- Create endless supply

That is just to name a few of solutions that are presently available to us right now. This does not mean though we will go with any of these. We feel it will be best if we wait and see in a couple of years what new things are possible with crypto.

Smaller blockchain size

We will be taking our currently blockchain and “resetting” it to no longer carry over 180GB of data.

Will I still be able to claim coins if I had bitcoin?

Absolutely. We will still be a fork of BTC, but we won't need to carry the massive amount of chain data that comes along with it. You will still be able to claim coins and import your private keys to move over addresses and claim coins.

Conclusion

It has been an awesome journey so far and we have determined that you, the users, love the idea of a mineable coin you can get interest on. We are always trying to improve upon this coin and we truly value the opinions of our ever growing community, so keep them coming! We look forward to the future with you all and happy staking!

Sincerely,

Aaron Mathis
Head of Development
Bitcoin Interest