Hush Version 3
Pre-Release Version

Duke Leto[†]

April 10, 2019

Abstract.

Hush originally was a source code fork of the **Zcash** 1.0.8 codebase. Hush was originally called ”Zdash” and is not a chain fork, Hush mined it's own unique genesis block.

...

Keywords: anonymity, freedom of speech, cryptographic protocols, electronic commerce and payment, financial privacy, proof of work, zero knowledge.

Contents 1

[†] duke@leto.net

1 Introduction

2 Things Staying The Same

- 21M total supply
- Block reward
- Block time
- Halving interval
- Delayed-Proof-Of-Work

3 Things Changing

- New Genesis Block
- Sprout Disabled
- First Pure Sapling Chain, with Super Fast Shielded Transactions
- s/ZEC/KMD/ as upstream
- New main Github repo
- Addition of 10% Founders Reward
- Address prefix change (t1,t3 becomes R,b)
- RPC and P2P ports
- Enable CryptoConditions (Custom Consensus)
- Block Size increase to 4MB
- Shielding Rule
- TLS Support

4 Hush v1-v2 Total Supply Bug

The original Hush devs added the original pre-mine in such a way that Hush would have a supply greater than the intended 21,000,000 after about 30 years. This fact was discovered in the process of emulating the current Hush supply curve (halving interval) on our new Komodo-based chain. This bug will be corrected on our new chain (Hush v3) by ceasing block rewards when total supply hits 21M coins, as intended.

As a reminder, NONE of the current Hush team received any the original 0.76% (160,000 HUSH) pre-mine. All of the original Hush developers who received the reward have long since left the project.

The current Hush chain (version 2) will attain a supply of 21,000,000 coins at Block 5922239 which will have a Block Reward of 0.09765625 HUSH. This happens between the 7th and 8th halvings.

But because the original devs of Hush added a pre-mine of 160,000 HUSH in blocks 1 through 4, the current Hush supply curve will continue past the 21M supply mark until Block 26039999 when supply is 21159937.4895 HUSH and the last block reward of 1 satoshi is awarded just before the 31st halving.

The core issue is that blocks 1 through 4 had a block reward of 40,000 each instead of 12.5 each in the GetBlockSubsidy() function defined in main.cpp, but the overall emission schedule was not modified to take this into account.

This mistake would eventually lead to an extra 159,937.4895 HUSH of total supply beyond the intended totaly supply of 21M, which would happen after about 30 years, between the 7th and 8th halvings.

This bug in the supply curve of Hush will be fixed during the migration to a Komodo asset chain, where we can use ac_end=N to specify a block when block rewards should cease. This will allow us to enforce the intended 21M total supply of Hush.

To calculate the value of ac_end for the new Hush chain:

ac_end = 5922239 - (number of blocks in old Hush chain) - (zero block reward transition period) ac_end = 5922239 - 500000 - 128 ac_end = 5422111

To clarify, Hush will have a consensus rule that block rewards stop at block 5422111 which will enforce a total supply of 21M coins.

5 New Blockchain Size

The Hush blockchain will essentially be compressed, down from its current size of about 3.4GB to a few megabytes. This is related to the fact that there are about 30,000 unique addresses on the Hush blockchain which contain funds.

This compression will greatly improve the user experience of new Hush users, which can install and sync a full node in just a few minutes.

6 Special Thanks

Special thanks to jl777 and the greater Komodo community for inspiring a new generation of cypherpunks to innovate outside the constraints of Bitcoin and Zcash core communities.

Special thanks to radix42, Savior Of The Memo Field, for mentoring me in my early days as a cryptocoin dev.

Remember, remember, the 5th Of November.

7 References