# Hush Version 3
## Pre-Release Version

Duke Leto[†]

April 13, 2019

**Abstract.**

**Hush** originally was a source code fork of the **Zcash** 1.0.8 codebase. Hush was originally called "Zdash" and mined a genesis block on Nov 17, 2016. The latest version of **Hush** migrates to a new codebase with a new genesis block while keeping the emission schedule as close as possible to the original intentions

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

## Contents

1

1 Introduction 3

2 Things Staying The Same 3

3 Things Changing 3

4 First Pure Sapling Blockchain 3

5 10% Founders Reward 4

6 New Upstream: KMD 4

7 CryptoConditions 4

8 Hush v1-v2 Total Supply Bug 5

9 New Blockchain Size 5

10 Delayed Proof-Of-Work 6

11 Cryptopia Attack 6

[†] duke@leto.net

12 Special Thanks 6

13 References 6

# 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)
- Improved Difficulty Adjustment Algorithm (LWMA-jl777)
- Block Size increase to 4MB
- Shielding Rule
- TLS Support

> Governments can be useful to the governed only so long as inherent tendencies toward tyranny are restrained. - The Stolen Journals

# 4 First Pure Sapling Blockchain

HUSH is proud to be the very first pure Sapling blockchain! HUSH enables Sapling at Block 1, which means no Sprout UTXOs will ever exist on our new blockchain. This removes any future risk of Sprout bugs/CVEs and drastically reduces the maintenance cost going forward, as Sprout code and Sapling code are different codepaths and so supporting Sprout at least doubles the amount of code to maintain.

No other blockchain has started as a pure Sapling chain, all other existing Zcash source code forks have transitioned from Sprout to Sapling.

## 5 10% Founders Reward

HUSHv3 adds a 10% Founders Reward, in perpetuity, until block rewards end. This is approximately 5.5 million blocks or about 30 years.

The Founders Reward is paid out every block in vout

1

to a single address of type "pubkeyhash":

RHushEyeDm7XwtaTWtyCbjGQumYyV8vMjn

with scriptPubKey

76a9145eb10cf64f2bab1b457f1f25e658526155928fac88ac

Initially the Founders Reward is 1.25 HUSH, starting at Block 129 until the first halving on the new chain at Block 340000.

In order to help transition, there will be a period of 128 blocks of zero block reward, which enables the new mainnet to be started just before our snapshot block, ready for miners to switch over. This also allows mining necessary blocks to start the chain and dispersing funds without developers unfarily earning many of the early block rewards. This corresponds to roughly 6hrs but our block times are not expected to converge to 150 seconds for a few days, so it is a rough estimate.

## 6 New Upstream: KMD

HUSH is no longer directly a source code fork of Zcash (ZEC), it is now a fork of Komodo (KMD). Since KMD itself is a fork of ZEC, this means we gain an immense amount of code and features, and all the development velocity of jl777. As an example, during the development of HUSHv3, over the course of a few weeks, about 20,000 lines of code was changed in upstream Komodo repo, adding many features and fixing various bugs.

We expect to see the developement velocity of the HUSH community greatly increase, since we will now essentially have jl777 constantly doing low-level blockchain internals coding, which frees up other developer resources to work on wallets, explorers, HushList protocol and applications which sit on top of the RPC interface.

HUSHv3 is a source code fork of the jl777/komodo git repository and live at

https://github.com/MyHush/hush3

As of Block 500,000, the legacy Hush network and codebase is unsupported. The network is not being forcibly turned off, those that want are free to use it, and use any encrypted data they may have in memo fields.

## 7 CryptoConditions

CryptoConditions are UTXO-based smart contracts and also an IETF standard:

https://tools.ietf.org/html/draft-thomas-crypto-conditions-04

Hush will enable the following CryptoConditions initially, and plans to enable others as time goes on:

- Heir - cryptocoin inheritance
- Gateway
- Oracle
- Channel

- Faucet

These features will allow for an entire ecosystem of decentralized applications (dApps) to be built on top of HUSH, which integrate with HushList protocol as well as cross-chain integrations with other Komodo asset chains, such as BTCH, ARRR or various others.

# 8 Hush v1-v2 Total Supply Bug

> To save one from a mistake is a gift of paradise. - Stilgar to Lady Jessica

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

TODO: deal with asset magic epsilon, which could be up to 10? blocks of BR average case it will be 5 blocks, worst case 10, so 5422101 would enforce just less than 21M

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

# 9 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.

## 10 Delayed Proof-Of-Work

> May thy knife chip and shatter. - Fremen saying of ill will against an adversary

HUSH will continue to have Delayed Proof-of-Work as protection against 51% attacks and double spend attack prevention. No other technology is proven in production like DPoW.

The current implementation of DPoW in Hush v2 was tested in a test attack. A large amount of hashrate was rented at NiceHash, and a 51% attack was attempted, which would re-organized a notarized block. The attack repeatedly failed and wasted a large amount of BTC of the simulated attacker.

HUSHv3 will be migrating to the core DPoW implementation of Komodo itself, instead of relying on the implementation that was ported from Komodo to the Hush v2 codebase. This further increases HUSH development velocity and reduces our maintenance burden to merge upstream code.

## 11 Cryptopia Attack

## 12 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.

## 13 References