Hush Version 3
Pre-Release Version

Duke Leto[†]

April 19, 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 based on Komodo and Zcash 2.0.x with a new genesis block while keeping the emission schedule as close as possible to the original intentions.

> A beginning is the time for taking the most delicate care that the balances are correct.
> – "Manual of Muad'Dib" by the Princess Irulan

Keywords: anonymity, freedom of speech, cryptographic protocols, electronic commerce and payment, financial privacy, proof of work, zero knowledge zkSNARKs, HushList, cryptoconditions, smart contracts, 51% attack, double spend attack.

Contents

[†] 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 Sprout-Free Chain, with Only Sapling 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 Sprout-Free Sapling Blockchain

HUSH is proud to be the very first blockchain to enforce only Sapling transaction from the very beginning! 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.

Most closely aligned to Hush is our sister coin Pirate (ARRR), which was the very first coin to disable normal transparent transactions (only coinbase and notarizations) and was one of the first coins to transition away from Sprout to Sapling. The decision for HUSH to disable support for old Sprout coins, after a certain block height, was inspired by Pirate: https://pirate.black

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 lives 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 that have cryptoconditions enabled.

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

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 first DPoW transaction occured at Apr 14, 2019 10:38:10 PM Eastern Time on the new HUSH mainnet :

https://explorer.myhush.org/tx/e73105092bbf01694af250f8ef89aa38d955856a5a3496e3336eaca59492b29f

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

Delayed-Proof-of-Work had been implemented in Hush in early 2018 but took many months to finish testing and be pushed to mainnet. During this time, an enterprising attacker probably saw that their window to attack HUSH was closing.

This attacker performed a series of 51% and double spend attacks against Cryptopia, between August 28th and September 21st 2018 It was designed to use amounts small enough to evade daily limits or fraud detection.

There were dozens of block reorganizations longer than branchLen=2, the largest being a reorganization of:

> At Fri, 21 Sep 2018 07:00:50 GMT the 46 block subchain:
> 00000009abdccd07615216765b17f99fbfc50e4106efe7bee2e4ca22810b0fa3..
> 000000028afb1daccbd0ac17d8685deeb0d072fdc5d4609209dd68675f873611
> was orphaned and replaced by the 45 block subchain:
> 00000009abdccd07615216765b17f99fbfc50e4106efe7bee2e4ca22810b0fa3..
> 000000038aadc3d77ae6df320e51168e6215f9abe62b65b51633715f719773bc

Note that the above block hashes must be looked up on a legacy HUSH block explorer such as https://explorer.hush.zelcore.io and additionally, the orphaned block will not be in the main chain and only will exist as an orphaned block on nodes which originally saw that invalidated chain.

Via blockchain analysis and detailed transaction logs from Cryptopia, who gave us details about which addresses the attacker was using, it was determined that the following addresses are owned by the Cryptopia Double Spend Attacker, with old HUSH v2 addresses on the left and new HUSH v3 addresses on the right.

> 651000 HUSH t1bEBr1LdBQtHun7B5L82R65FgpWyyWFx8L = RSdmvBomouuGP9RUc5J2NoJYCRnVqT3j5V[redacted]
> 29279.8 HUSH t1KttMaacGw17oFitV448TGfwM2yovm4g6Q = RBJURm3kuS26Gd3C1oE8QyuDreFKpkNT2Z[redacted]

These two addresses own a total of 680,000 HUSH which was not dispersed to the equivalent addresses on the new HUSH v3 mainnet. These funds currently remain in the HUSH Founders Reward wallet and will be used to reimburse all who were stolen from at Cryptopia, which will enable HUSH trading to resume. Any remaining funds will be used for additional exchange listings.

12 Immutability of HUSH v2 + v3

Please note that the immutability of the legacy Hush mainnet or new Hush v3 mainnet was never compromised. The Bitcoin Protocol was observed strictly and Hush did not do what other coins have done in similar situations

which is to actually backdoor the Bitcoin Protocol itself, and make it such that certain pubkeys can make transactions which they shouldn't, to spend funds which were lost or stolen, etc. This was deemed unacceptable, for obvious moral, security and financial reasons.

Instead, we have chosen to keep our original intentations, which is that we do not believe that forcibly turning off peoples nodes is right. So people on the legacy Hush chain are free to continue using it. They should note, that the Sprout Inflation bug is still waiting to be exploited there and that DPoW is no longer active (the last notarization was Block 501080), so 51% attackers have a playground.

Every user of Hush gets to decide if they choose to keep using the v2 or v3 chain and no user is forced to use either. This way embraces decentralization at the very core, since we do not force our choices upon our users. They get to decide which chain goes forward.

13 Sprout Inflation Bug Playground

Let it be known that HUSH v2 mainnet is considered a Sprout Inflation bug playground, and there is a bounty of 500 HUSH for a script which makes it trivial to exploit the Sprout inflation bug and generate arbitrary amounts of funds insize of a Sprout zaddr.

Developers and information security researchers are directed here for more info:

https://github.com/MyHush/hush3/issues/7

14 Dispersing Funds To The New Mainnet: Swapping Airdrop

This process is sometimes called an "airdrop" because the technical process of sending funds to addresses is the same, but HUSH v3 is technically a "coin swap", since we do not support our legacy chain.

A total of 3127 transactions with "sendmany" were made to complete sending funds to 31,000 unique addresses which contained funds on the Hush v2 blockchain as of the snapshot block of 500,000. The average address had about 200 HUSH while the median address had 1 HUSH.

This data was extracted via the "getsnapshot" RPC which I helped write for Komodo and ported to Hush v2. Additionally I ported the -stopat CLI param from Komodo to Hush v2, so that the full node could be stopped at an arbitrary block height while still able to answer RPC requests.

Full data is available here:

https://github.com/MyHush/hush3/blob/duke/contrib/snapshot/snapshot_500000.json

The actual script used to disperse funds can be found here:

https://github.com/MyHush/hush3/blob/duke/contrib/snapshot/airdrop_hush3.sh

15 Shielding Rule

Previously Hush inherited the rule about shielding coinbase before sending to a transparent address. Now that Hush is based on Komodo, this rule no longer exists, which means mining pools can send newly mined coinbase funds directly to pooled miners.

The rule was well-intentioned, but it did not result in real privacy improvements, since 95% of all ZEC is still in transparent addresses, and people move amounts "throught" zaddrs (instead of keeping funds in them) in such a way as to make transactions easy to link.

Hush will take the stance of educating users to the risks of transparent addresses, constantly, and make shielded operations the default in all GUI wallets.

Additionally, since shielding is so fast now, and various service providers are now supporting Sapling shielded addresses, we encourage users to hold funds in Sapling zaddrs by default and only use transparent addresses when necessary, such as exchanges that only support transparent addresses.

16 Sapling-Enabled HushList

...

17 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 Core and Zcash Core communities.

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

Special thanks to Satoshi Nakamoto for starting all this fun.

18 References