Bitcoin Hush (**BTCH**) Cryptocoin Specification
Pre-Release Version

Duke Leto, jl777

January 23, 2018

Abstract.

Bitcoin Hush (**BTCH**) is a new research and development cryptocoin which has many unique features compared to existing options. It avoids all transaction history and simply imports Unspent Transaction Output (UTXO) values for four different blockchains onto a fifth "host chain", Komodo. We use the Komodo Asset Chain feature to build a coin with delayed-Proof-of-Work, which enjoys the full security of Bitcoin level security via notarization.

Additionally, the need for the latest two way replay protection (2WRP) algorithms are completely avoided, since no transaction hashes are leaked onto the new chain. This also completely avoids the problem that many Bitcoin forks have where they inherit a very large existing chain and must sync gigabytes of data.

We hope these techniques are utilized in all future Bitcoin and related forks to avoid large inefficiencies as well as potential replay attacks.

The recently released **HushList** protocol is compatible with **BTCH**, **KMD** and all **KMD** asset chains, which all contain *zk-SNARK* technology. Additionaly, **HushList** is known to be compatible with **HUSH**, **ZEC**, **ZCL**, **ZEN**, **ZER** and the upcoming **BTCP**.

This specification defines how the **BTCH** cryptocoin works and how how it builds on the foundation of **Komodo**, **Zcash** and **Bitcoin**.

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

Contents