



# Take Back Your Privacy With Hush

Duke Leto  
[duke.letto.net](https://duke.letto.net)  
[hush.is](https://hush.is)

# What Is Hush?



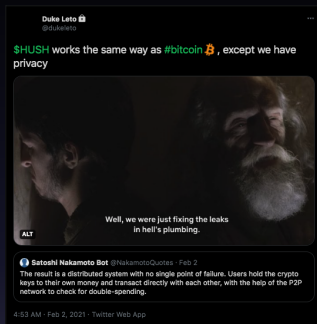
- Magic Internet Money
- Private Chat Platform
- Store-of-Privacy

# How Is Hush Like Bitcoin?

```
// Copyright (c) 2009-2010 Satoshi Nakamoto
// Copyright (c) 2009-2014 The Bitcoin Core developers
// Copyright (c) 2016-2020 The Hush developers
// Distributed under the GPLv3 software license, see the accompanying
// file COPYING or https://www.gnu.org/licenses/gpl-3.0.en.html
*****
```

- Based on Bitcoin 0.11.2
- No Company, Decentralized Community
- 21M Total Supply
- Halvings every four years
- Hush extends Bitcoin Protocol
- Mine with ASICs
- wallet.dat works very similar
- Compatability at many layers
- Store-of-Value  $\implies$  Store-of-Privacy

# How Is Hush different?



- Alice sends Bob money
- Alice's address is private!
- Bob's address is private!
- The amount sent is private!
- Encrypted memo field is private!
- The number of recipients is private!
- Plausible Deniability

# How Is Hush different?

You must use privacy, it's no longer optional!



- Everyone must use privacy, no choice
- Best practices are automated
  - Only can send to a zaddr (z2z)
  - Send to multiple addresses (Sietch)
  - P2P encryption mandatory (TLS 1.3 Only!)
- How much money was sent?
- How many people received funds?
- Was encrypted additional information sent?
- "Herd immunity" to metadata attacks

# Zcash "Privacy"

**Design new Elliptic Curve  
using Barreto-Naehrig  
construction**



**Implement new zk-math  
in efficient Rust code with  
memory-safety guarantees**



**Optimize shielded Sapling  
addresses to be fast as hell  
and use very little RAM**



**Allowing transparent addresses  
as the default transaction type**



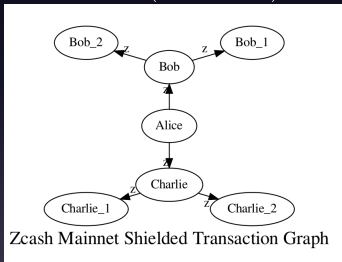
**The Zcash Mind Prison Clown**

Invented new Zero-Knowledge math but don't use it!!!

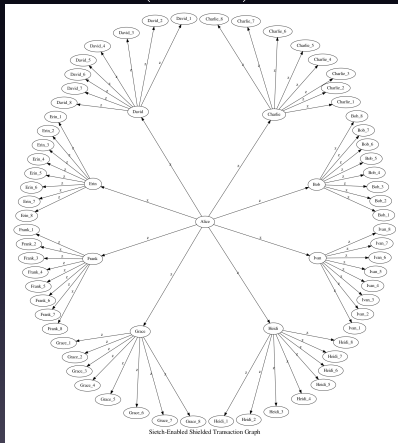
## Sietch

attackingzcash.com

Zcash z2z (optional)



Hush z2z (always)



An underground fortress for every transaction!

# If You Are Not Paying For Privacy...

You Don't Have Any!





# How Is Hush different?

explorer.hush.is

explorer.hush.is

[Hush](#) | [Explorer](#) | [Twitter](#) | [Telegram](#) | [Telegram\\_Support](#) | [Telegram\\_Mining](#) | [Reddit](#) | [YouTube](#) | [BitcoinTalk](#) | [Mastodon](#) | [Matrix](#)

## HUSH Blockchain Explorer

[Blocks](#) | [Addresses](#)

Block Height	441967
Block Hash	00000018Feed8ecdFb05cb1a7675Se26a00d6316dbca9b2cf42b1449a504f898
Longest Chain	441967
Chain Tip Time	Sun Feb 28 02:57:10 2021
Total Transactions	761844
Transaction Rate	1.0000 per minute (Monthly Avg)
Difficulty	9161003
Network Solution Rate (Hashrate)	1.80 MegaSols/s
Circulating Supply	10745642.68612515 HUSH
Shielded Supply	4411420.49834931 HUSH
Percent Shielded	41.053 %

- Extreme Privacy Block Explorer
- No Javascript (client or server)
- No Images (web bugs)
- Tor Hidden Service Available
- Doesn't doxx you

# How Does Hush Build Upon Bitcoin?

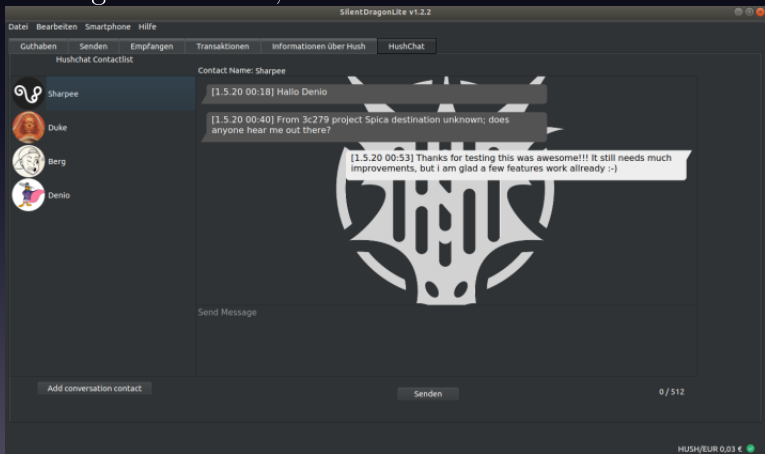
Hush is at Layer 2, with Lightning Network and Bisq







- Sender, receiver, amount are PRIVATE
- Encrypted p2p connections with TLS 1.3
- ...

# What Is HushChat?

HushChat is an encrypted chat messaging protocol and decentralized platform. It's ideas are based on Signal Protocol, but without all the bad stuff.



# What Is HushChat?

	 Hush	 Signal	 wickr	 Threema <small>Secure Group Messaging</small>	 WhatsApp	 Telegram
Open Source Client and Server	✓	✗	✗	✗	✗	✗
E2EE 1-1 and Group chats	✓	✓	✓	✓	✓	✗
No Phone number or Email registration	✓	✗	✓	✓	✗	✗
Onion routing/IP Address masking	✓	✗	✗	✗	✗	✗
Decentralised Servers	✓	✗	✗	✗	✗	✗

- HushChat Protocol is an encrypted chat messaging protocol and decentralized platform.
- Inspired by Signal Protocol, without the bad stuff.
- We don't use Signal code.
- Proud libsodium user! Unlike Zcash...

# What Is HushChat?

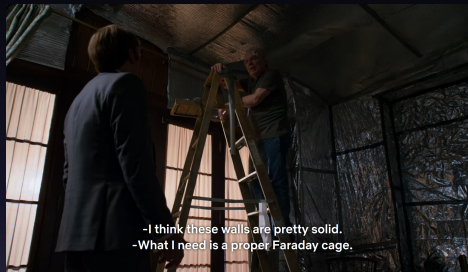
## Signal

- Signal Protocol
- Centralized
- Phone Numbers
- Closed Source Server
- Uncle Sam backdoors

## HushChat

- HushChat Protocol
- Decentralized
- Shielded Addresses
- GPLv3 Free Software
- ??? backdoors?

# Who Profits From Surveillance?



- MFAANG  
(MSFT,FB,Amazon,Apple,Netflix,Google)
- Surveillance Valley (Silicon Valley)
- Governments
- Militaries
- Advertisers

# Who Spies On You?

Depends on your GPS coordinates... TLDR: Too many people, alphabet soup.

## Country

- Australia - ASIO
- Canada - CSE
- China - MSS
- England - GCHQ
- France - DGSE
- Germany - BND
- USA - NSA
- Russia - FSB (ФСБ)
- Singapore - ISD
- Spain - CNI
- Switzerland FIS

## Global Networks

- Five Eyes (FVEY)
- Nine Eyes
- 14 Eyes
- FATF  
(China+USA+Russia!)

# Surveillance Devices

Most tech is designed to surveil and eject metadata in all directions.

You give it for free and it's sold back to you and others.

- "Party Lines"
- Fax machines
- Email
- Mobile Phones (SMS especially)
- Web browsers
- Web servers
- Social Media
- Every for-profit tech company



# Hush Is Human Rights

United Nations

Universal Declaration of Human Rights

Most governments have not signed this into law.

Code is law on the HUSH blockchain!

**Article 12.**

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

No government or company can see inside your encrypted data! TODO: seems crazy meme

# Silicon(?) Valley

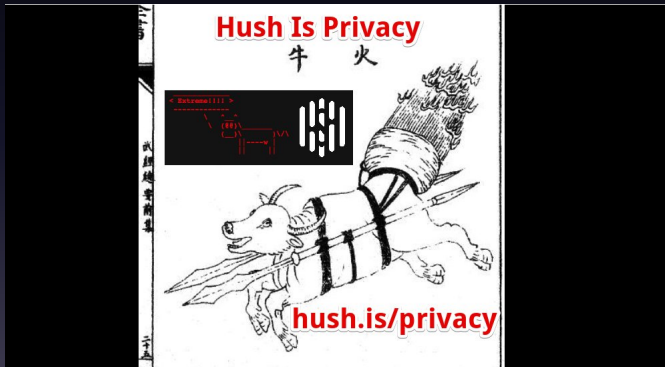
Actually, it's Surveillance Valley.

Started by two Stanford professors who encouraged students to start companies

- Best academic research was monetized
- Students invented efficient spy planes
- Spy planes prevented deaths
- Spy submarines don't require boots-on-the-ground
- Some PhD theses were Top-Secret!
- These students went to form the first SV companies
- Example: Hewlett-Packard
- Now these few companies own all your data

# Hush Is Privacy

Hush delivers privacy in a world of surveillance



# What Data Do They Want?

Stop helping the surveillance companies!

Used To Be...

- GPS
- IMEI
- IP address
- Browser details
- Website URLs
- Emails
- Facebook messages

But now it's...

- GPS
- IMEI
- Financial records
- Shopping preferences
- "encrypted" chats
- 24/7 camera feeds
- Voice recordings
- Genetic samples +  
Medical records

# Hush Is Privacy

Must trust the hardware and software!



# Always-On Privacy By Default

## Bleeding-edge Peer-to-Peer (p2p) Encryption

- Transport Layer Security (TLS) 1.3 only!
- Unencrypted connections disallowed
- Advanced peer banning tech
  - Feeler connections
  - test-before-evict
  - REFERENCE
- Erebus Attack mitigation via ASN map

# Erebus Attack

<https://erebus-attack.comp.nus.edu.sg>

Muoi Tran, Inho Choi, Gi Jun Moon

Anh V. Vu, Min Suk Kang

## Recent Attack against Bitcoin

- Research by National University of Singapore
- Bitcoin Core realizes it's important
- Code remains unmerged on Github for 1.5yrs
- Likely never turned on by default
- Hush protects all users by default already
- Very first cryptocoin (and privacy coin) to do this

# Attacks That Molded Hush

Every attack makes Hush stronger.

- Cryptopia 51% attacker  $\implies$  DPoW
- Sprout Inflation Bug CVE  $\implies$  Sapling
- KMD malicious DPoW Attack  $\implies$  Hush DPoW



# Delayed-Proof-of-Work

Big blockchains can protect little blockchains.  
It only makes sense to be protected by the strongest:  
Bitcoin

- HUSH injects blockhash data into HUSH+BTC
- This costs HUSH+BTC, constantly
- HUSH is protected by hashrate of BTC
- Any other coin can jump in our wagon
- Drastically easier/cheaper than doing it yourself
- Cost is \$1K USD in BTC or XMR per month
- Solves "Double Spend" attacks on exchanges!

# Delayed-Proof-of-Work

DPoW enforces censorship-resistance.  
Without DPoW, a mining attacker can rewrite history, like politicians.

- DPoW means your data cannot be removed
- DPoW means an attacker needs to attack BTC
- Attacks are extremely costly
- Attacks are less likely to succeed
- Attackers cannot profit so go elsewhere

# Hush + Tor

## Evolving greatly in 2021

- Tor Network is under Attack
- v2 Hidden Services being DoS'ed
- Migrating from v2 to v3 Hidden Services
- Tor turning off v2 in Oct 2021
- Bitcoin recently enabled v3 support
- Currently being ported to Hush

# zaddr opsec

- One zaddr per
  - Exchange
  - Mining Pool
  - Online Seller
- When in doubt: new zaddr
- Don't post publicly
- Only senders need to know a zaddr
- What about donation zaddrs?

# Donation zaddr opsec

This mitigates attacks from those that know your zaddr and require your wallet online to be attacked.

- Create a brand new wallet
  - SDP is best (most isolated)
  - Or SD, then SDL
- Keep donation zaddr offline!
- Make viewkey if desired
- Only put wallet online to spend
- NEVER use a public donation address for anything else
- BIP47  $\implies$  HIP47 will greatly improve this

Or just #yolo

# Erebus Attack Prevention

- Hush filters peers by ASN
- Bitcoin uses Class B (/16)
- 65000 vs 7.4M buckets
- SilentDragon Peers Tab show ASN

# Privacy: Consensus Layer



After 4 years...

- Zcash (optional) - 6%
- Hush (4 months after z2z) - 41%

Zcash (ZEC) mainnet is a privacy disaster.

# Privacy: Consensus Layer



Zcash optimizes for profit, not privacy.



# Privacy: Consensus Layer



Multiple Analysis companies now support Zcash!

# Use Cases

- Censorship-resistant Will + Testament
- Medical billing
- Lawyer-client secure chat
- Censored Journalist

# Hush Finds Exploits and Bugs Constantly

If we make fun of your favorite things, it's probably because it's trivial to exploit or has no privacy.



# Hush Finds Exploits and Bugs Constantly

- "Attacking Zcash Protocol For Fun And Profit"
- [attackingzcash.com](https://attackingzcash.com)
- CVE-2019-11636 (Sapling Woodchipper)
- CVE-2019-16930 (PING/REJECT)
  - Discovered by Dan Boneh (Stanford)
  - Reported privately to Zcash
  - Zcash created update with no explanation or binaries
  - I reverse engineered from code
  - It was trying to be hidden
  - Zcash CEO/CTO/CSO blocked me on Twitter
- CVE-2021-????? (OPIP)

# How To Get Some HUSH?

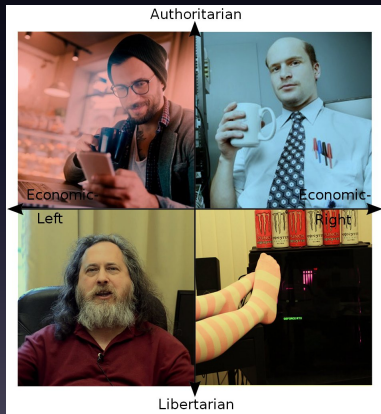


From most privacy to least privacy.

- Join our community, do work, get paid in HUSH
- Purchase on Decentralized Exchange (DEX)
- Mine HUSH via purchasing ASICs
- Mine HUSH via renting hashrate
- Purchase on Centralized Exchange
  - HushDEX

# Join The Hush Community

Most types of Hackers and Cypherpunks welcome



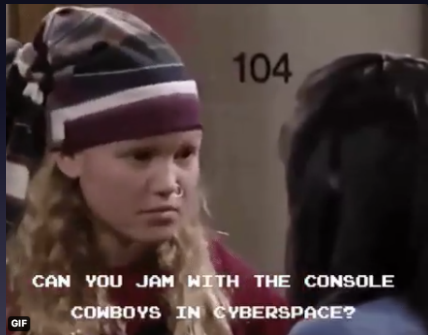
- We already abandoned Slack+Discord
- Official Telegrams
- English: [hush.is/tg](https://hush.is/tg)
- Russian: [hush.is/tgru](https://hush.is/tgru)
- Chinese: [hush.is/tgzh](https://hush.is/tgzh)
- Spanish: [hush.is/tges](https://hush.is/tges)



# Join The Hush Community

If you know about this stuff  $\implies$  earn HUSH

- Linux/BSD servers
- C/C++
- Rust
- Docker
- QT5
- Android/Kotlin
- Tor/i2p/Mix networks



# Thanks!

Vintage Duke meme



In Zdust We Trust