



Take Back Your Privacy With Hush

Duke Leto
duke.letto.net
hush.is

What Is Hush?



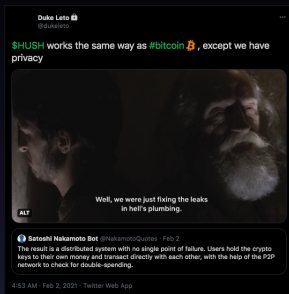
- Magic Internet Money
- Private Chat Platform
- Store-of-Privacy
- mainnet launched 2016
- Global Community
- i18n ~ 20 langs

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
- Compatibility 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
- 75 seconds vs 10 minute blocktime

Bitcoiners Pay Extra For Privacy



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

How Is Hush different?

Herd immunity is network-wide resistance to metadata attacks.



- Sietch adds non-determinism
- Your neighbor isn't doxxing you all day
- You are responsible for your privacy, not others
- Privacy increases with time, anonset \uparrow
- XMR anonset is per-tx (small), decreases w/ time
- HUSH anonset is network-wide
- HUSH anonset is non-decreasing on average
- HUSH anonset \gg ZEC anonset
- HUSH: 1st privacy coin w/ real-time anonset stats

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**

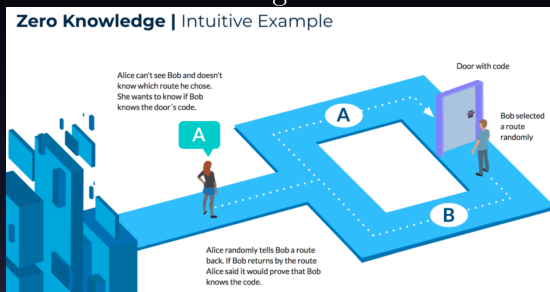


The Zcash Mind Prison Clown

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

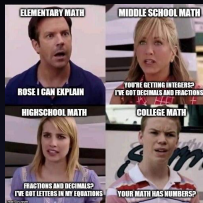
Hush Zero Knowledge Math

The Magic Sauce



- Zero Knowledge Proofs
- Invented in 1985, just became "usable"
- zk-SNARKs (close to 100 kinds)
- Zero Knowledge Succinct Non-Interactive Arguments of Knowledge
- Prove X is true, without saying anything about X
- Elliptic Curves, Fields, Group Theory

zk-SNARKs



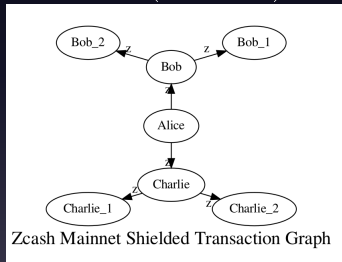
New atom for building privacy software

- One "flavor": Zcash Protocol built on them
- Monero uses older math that leaks metadata
- There are others, like zk-STARKs/etc
- Hush Protocol is an improved Zcash Protocol
 - Same exact cryptographic primitives
 - We enforce their use
 - First blockchain to use Sapling zaddrs exclusively
 - All our privacy is inside one "pool"

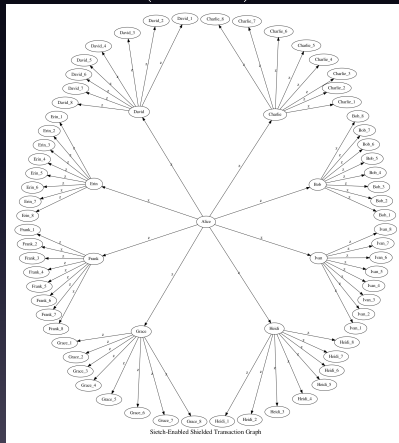
Sietch

attackingzcash.com

Zcash z2z (optional)



Hush z2z (always)



An underground fortress for every transaction!

Sietch

Attacking Zcash Protocol For Fun And Profit
Whitepaper Version 0.6Duke Leto + The Hush Developers¹

February 9, 2021

Abstract

This paper will outline, for the first time, exactly how the **ITM Attack** is linkability attack against shielded transactions works against Zcash Protocol and how **Hush** is the first cryptocoins with a defensive mitigation against it, called **Sietch**. Sietch is already running live in production and undergoing rounds of improvement from expert feedback. This is not an academic paper about preprints. It describes production code and networks.

We begin with a literature review of all known metadata attack methods that can be used against Zcash Protocol blockchains. This includes their estimated attack costs and threat model. This paper then describes the **ITM Attack**, which is a specific instance of a new class of metadata attacks against blockchains which the author describes as **Metaverse Metadata Attacks**.

The paper then explains Sietch in detail, which was a response to these new attacks. We hope this new knowledge and theory helps cryptocoins increase their defenses against very well-funded adversaries including nation states and chain analysis companies.

A few other new privacy issues and metadata attacks against Zcash Protocol coins will also be enumerated for the first time publicly. The ideas in this paper apply to all cryptocoins which utilize transaction graphs, which is to say just about all known coins. Specifically, the Metaverse Metadata class of attacks is applicable to all **Bitcoin** source code forks (including Dash, Verge, Zencoin, and their forks), **Cryptotele** Protocol coins (Monero and friends) and **MimbleWimble** Protocol (Grin, Beam, etc) coins but these will not be addressed here other than a high-level description of how to apply these methods to those chains.

In privacy ydust we trust.

If dust can attack us, dust can protect us.

- Switch Motus

Keywords: *anonymity*, zcash protocol, cryptographic protocols, zk-SNARKs, metadata leakage, de-anonymization, electronic commerce and payment, financial privacy, zero knowledge mathematics, linkability, transaction graphs, shielded transactions, blockchain analysis.

Contents**1 Introduction**

1

3

¹ hush.is, <https://github.com/dadadada>, F8E218F4C22F4615E6C73A4402E88E54403400Атакуюм Zcash Протокол Ради Забавы И Выгоды
Whitepaper Version 0.6Duke Leto + Hush Разработчики¹

7 марта 2021 г.

Краткий обзор.

Данный документ, впервые, описывает как именно работает **ITM Атака** (специализированная атака против защищенных транзакций) против Zcash Протокола и **Hush** как первого криптокоина, защищающего **Metaverse** - специализированного характера против такой атаки. Sietch уже работает в производстве, так же проходит этапы улучшения на основе отзывов экспертов. Это не научная статья и небытийное письмо. Документ описывает производственный код и сеть.

Мы начинаем с обзора упомянутой о атаке методов, которые могут быть использованы против блокчейнов Протокола Zcash. Далее включена стоимость такой атаки и модель угрозы. Документ далее описывает **ITM Атаку**, которая является конкретным примером нового класса или категории атак блокчейнов, которой автор описывает как **Metaverse Metadata Attacks**.

Далее далее описывает Sietch в деталях, что было ответом на подобные атаки. Мы надеемся новые знания и теория помогут криптокоинам увеличить их безопасность против очень хорошо финансируемых атак, включая национальные государства и компании, специализирующиеся анализом блокчейнов.

Несколько других новых проблем конфиденциальности и атаке методов против Протокола Zcash будут рассмотрены и описаны впервые. Идеи в этом документе применяются ко всем криптокоинам которые используют графики транзакций, что можно сказать про все известные криптокоины. И соответственно, конкретная атака Metaverse Metadata является для всех форков **Bitcoin** (включая Dash, Verge, Zencoin и их форки), криптокоинам Протокола **Cryptotele** (включая Monero) и монеты Протокола **MimbleWimble** (Grin, Beam, etc), но эти атаки не рассматриваются, только описаны обобщенно, как применить методы к их блокчейнам.

Мы верим в приватность dust.

Если dust (dust) может атаковать нас, dust может защитить нас.

- Sietch Motus

Keywords: *анонимность*, протокол zcash, криптографические протоколы, zk-SNARKs, утечка метаданных, деанонимизация, электронная коммерция и платежи, финансовая приватность, математика с нулевым разглашением, связываемость, графики транзакций, защищенные транзакции, анализ блокчейнов.

Содержание**1 Введение**

1

3

¹ hush.is, <https://github.com/dadadada>, F8E218F4C22F4615E6C73A4402E88E54403400

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

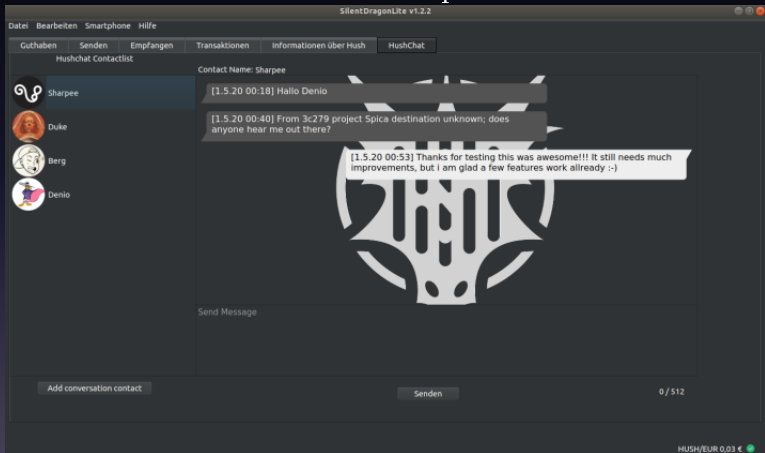


- Lightning Network
- Bisq Decentralized Exchange

We don't compete with Bitcoin, we build upon it.






What Is HushChat?

HushChat is an encrypted chat messaging protocol and decentralized platform.



Like Signal Protocol on a blockchain, with ratcheting.

What Is HushChat?

	 Hush	 Signal	 wickr	 Threema	 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.
- Signal Protocol with zaddr not phone numbers
- We don't use Signal code.
- Proud libsodium user! Unlike Zcash...

What Is HushChat?



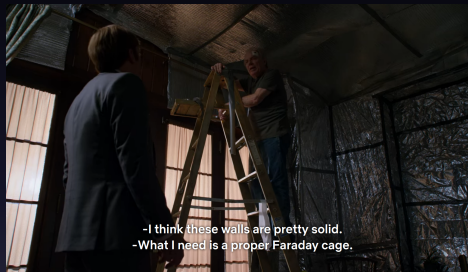
Signal

- 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

Backdoors Everywhere

Disagree? You probably get paid to cover up backdoors.

- Signal - Best Protocol, backdoored by USA
- WhatsApp - Backdoored by USA
- Wickr- Backdoored by USA
- Threema - Backdoored by USA
- Telegram - Backdoored by Russia
- WeChat - Backdoored by China
- Zoom/KeyBase - USA and China, most likely



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!)



A Rose By Another Name



- KGB \implies FSB

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/MMS)
- Web browsers
- Web servers
- Social Media
- Voice Assistants
- 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 multiple layers of encrypted data!



Silicon Valley?

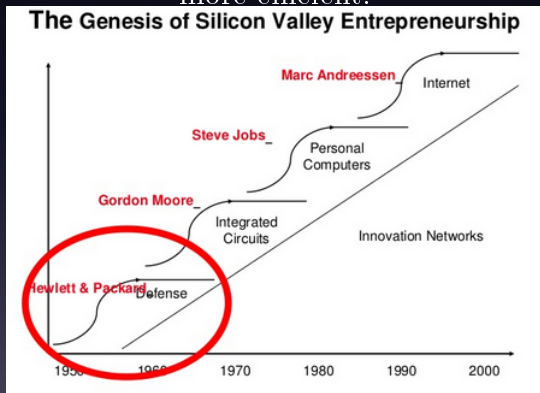
Started by two Stanford professors:

Terman (US) + Shockley (UK)

- Preferred Electronic Warfare (EW) contractor
- Best academic research was monetized
- Students invented/improved:
 - Efficient spy planes
 - Advanced Radar Jamming
 - Spy balloons, EME
 - Spy submarines
- Some PhD theses were Top-Secret
- Students went to form the first SV companies
- Example: Hewlett and Packard
- Example: "Traitorous 8 "
 - form Fairchild Semiconductor (1957)
 - 2 of 8 leave Fairchild to form Intel

Surveillance Valley

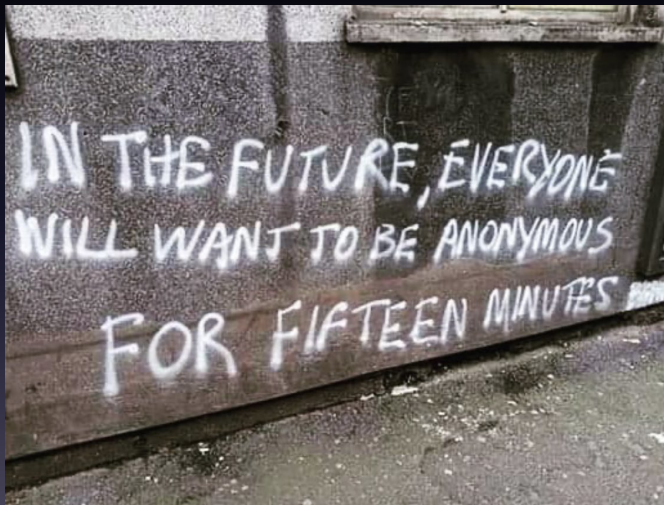
It's always been Surveillance Valley, from the start. Silicon made radar and radar jamming drastically more efficient.



steveblank.com/secret-history/

Hush Is Privacy

Humans had privacy by default 100 years ago.



Now we have surveillance by default.

Hush Is Privacy

Hush delivers privacy in a world of surveillance.



What Data Do They Want?

Anything they can use to control you, market to you and/or sell to others. Which is everything.

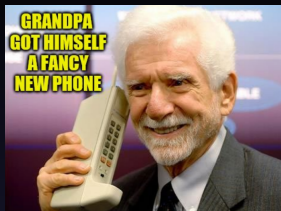
- GPS
- IMEI/IMSI
- IP address
- Browser details
- Website URLs
- Emails
- Facebook messages
- Shopping preferences
- Financial records
- "encrypted" chats
- 24/7 camera feeds
- Sentiment (reactions)
- Facial scans
- Voice recordings
- Genetic samples
- Medical records
- Biometric sensors

Hush Is Privacy

Must trust the hardware and software!



Hush + Precursor



HushDroid is cool, but still so many backdoors.
Precursor is amazing new mobile hardware!
Trustable hardware + zero-knowledge math privacy
⇒ Win



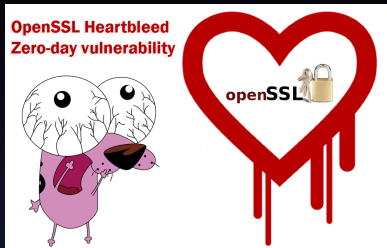
Precursor is the best HW in dev for use by Hush.

Privacy By Default

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

- Transport Layer Security (TLS) 1.3 only!
- Useless for surveillance coins, very important for privacy coins!
- Unencrypted connections disallowed
- Advanced peer banning tech
 - Feeler connections
 - test-before-evict
 - "Eclipse Attacks on Bitcoin's Peer-to-Peer Network"(2015)
 - Ethan Heilman* Alison Kendler* Aviv Zohar† Sharon Goldberg*
 - *Boston University, †Hebrew University
- BTC Core has implemented all countermeasures
- Erebus Attack mitigation via ASN map

Bleeding Edge of TLS



- NSA: TLS_AES_256_GCM_SHA384
- DJB: TLS_CHACHA20_POLY1305_SHA256
- No TLS certificates needed, that is a scam
- We deleted OpenSSL, now use WolfSSL!
- It's not made of CVE's
- Nodes non-deterministically prefer either cipher
- Forces network to use both ciphers randomly
- You cannot predict which will be used

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
- Fraudulent Exchanges (Graviex, Citex, etc)
- 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

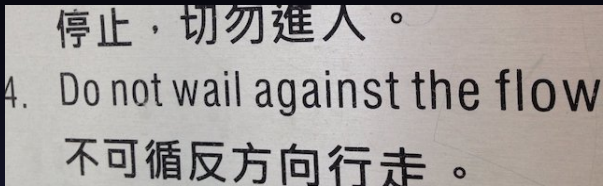
- HUSH injects blockhash data into HUSH+BTC
- This costs HUSH+BTC, constantly
- HUSH is protected by hashrate of BTC
- Any other coin can jump in our wagon
- Drastically easier/cheaper than doing it yourself
- Cost is \$1K USD in BTC or XMR per month
- Solves "Double Spend" attacks on exchanges!

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 they go elsewhere

Hush + Tor



Both evolving greatly in 2021

- Tor Network is under constant 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 shows ASN
- Shodan integration

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!

Hush Smart Chain (HSC)

Spin up a Hush-like network in 1 command

hush.is/hsc-creator

Let's create a HUSH Smart Chain!

You have great power at your fingertips! Use it wisely, for Good

Options

General

Customize general Hush settings

Fully Shielded ztz (-ac_private)



Name (-ac_name)

Initial Supply (-ac_supply)

Initial Block Reward (-ac_reward)

Block time (-ac_blocktime)

Block Halving Period (-ac_halving)

Public Key (-ac_pubkey)

Addnodes

Add trusted bootstrap nodes. Remove by clicking.



```
git clone https://github.com/hush/hush
cd hush3
./build.sh
cd src
./hush-smart-chain -ac_name=TUSH
-ac_supply=21000000 -ac_blocktime=60
-ac_private=1 -ac_reward=1250000000
-ac_halving=210000
```



Use Cases

- Lawyer-client secure chat
 - Enforced at protocol layer!
 - Dedicated HW as needed
- Censored Journalist
 - Encrypted data can be published
 - At a time determined later, or never
- Will + Testament
 - Encrypted Worldwide backup
 - Cryptographic proof
- International Diplomacy

Use Cases

International Diplomacy Requires Privacy

- China
 - Create their own HSC, requires National ID, biometrics + VPN
 - For foreign diplomats outside of China
- Russia
 - Create completely isolated chain for internal usage only
 - Requires being in secured physical locations
 - Can cryptographically prove who-did-what-when
- USA
 - Studies attacks on HUSH mainnet in a Faraday Cage Under A Mountain
 - So it can be used effectively, in the field, like Tor
 - Or attack it, if they need the lulz

Use Cases

International Diplomacy Requires Privacy

- Singapore
 - US+Russia+China decide to do cyberattack against SG
 - Most of the internet goes malicious
 - Tor+Hush allows SG diplomats to communicate with UN
 - They can provide cryptographic proof of data
 - UN could be a hub of diplomatic privacy
 - DPoW protects things from being erased from history books

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
- CVE-2019-11636 (Sapling Woodchipper)
- CVE-2019-16930 (PING/REJECT)
 - Discovered by Dan Boneh (Stanford)
 - Reported privately to Zcash
 - Zcash published weird emergency patch
 - Zcash had 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)

SilentDragon: SD

hush.is/sd

SilentDragon v1.2.0

Balance Send Receive Transactions Peers Market Feeds

Current Peers

PeerID	Address	ASB	TLS Color	TLS Verified	Is ban	Protocol Version	Prog. Time	Balance	Relay received	Relay sent
0	9c234973	TL513-4E21518-CCH-9H43364	False	KoBleerSendBroadcast:3.6.1V	1987420	0.000000	0	2289058	76985	
1	8c71916	TL513-CM0C84203-POX11391-9H43364	False	KoBleerSendBroadcast:3.6.1V	1987420	0.108669	0	1427618306	1701428	
2	4619418	TL513-4B43158-CCH-9H43364	False	KoBleerSendBroadcast:3.6.1V	1987421	0.032386	0	146470819	1701748	
3	46812	TL513-4E21518-CCH-9H43364	False	KoBleerSendBroadcast:3.6.2V	1987420	0.078276	0	141713195	1673077	
4	4651167	TL513-4E21518-CCH-9H43364	False	KoBleerSendBroadcast:3.6.2V	1987420	0.129183	0	219368936	2148208	

Balance

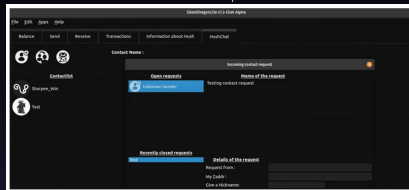
Address	Balance
Balance total	

Synchronizing (1194305/141276) Lag: 196306, Height=0,000000003 BTC

- Full Node GUI Wallet
- Downloads gigabytes of data
- Highest privacy

SilentDragonLite: SDL

hush.is/sdl



- GUI Lite Wallet
- HushChat GUI
- Encrypted wallet on disk
- Downloads megabytes of data
- Easiest for users
- Relies on external servers!
- Communities encouraged to run servers

SilentDragonPaper: SDP

hush.is/sdp

Speak and Transact Freely

Private Cryptocurrency and Messenger on Zero Knowledge Proof Encryption



HUSH Address

ze1007eudgvrvevjpdaxgskvzy2g8d45tws6sh
40vqey3wf7prj2q9wbcf0enavxq5p675qq22k5e

Private Key

```
secret-extended-key-main1qdr8et56qppqqrkq7w
la5836y2p9j2cnrueh86fwlhd8dpefn5lqprxanlxdj3e
4r02yn5c8tmaxa3e8h2hg9j5vovw6cf7j04d3ug7q4qk
j101lan0edc9q9qhd9nrmw1vada78j0229q9p0e0d3
1mex70rvudca9ph9d09karjxp6drv7h2x6cxwfwakho2
59rkr0w4kz35a6ahf0y43q9aift74haeck32bwefl0cfx
20x050p7eshrx6eqrua7ea56sacya61n
```

HUSH Address

ze1007eudgvrvevjpdaxgskvzy2g8d45tws6sh
40vqey3wf7prj2q9wbcf0enavxq5p675qq22k5e

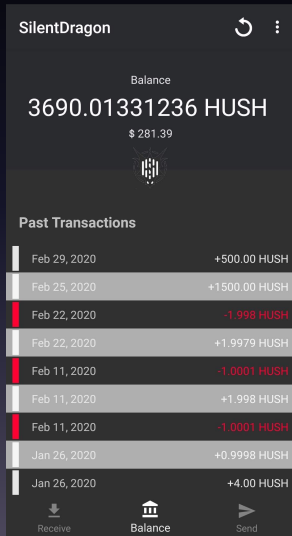


Page 1 of 1

- GUI Paper Wallet
- Generate addresses offline
- Print out QR code backups
- No bandwidth required
- Cold wallets

SilentDragonAndroid: SDA

hush.is/sda



- Android Wallet
- Pairs to SD or SDL
- "Lite mode" Coming Soon
- Like a mobile SDL
- On Google Play

Invest In Privacy



- HUSH is a Store-of-Privacy. You can purchase privacy now and save it for use in the future, when privacy is more costly.
- Monero and Zcash are over 1000x times more expensive than HUSH, but provide drastically inferior privacy!
- Zcash is funded by Surveillance Valley investors.
- Monero (XMR) has over 90% of total supply mined already while HUSH has about 50% mined. HUSH is a fairer emission schedule.
- Same emission as BTC: halvings every 4 years

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)
- Solo Mine HUSH via ASICs
- Solo Mine HUSH via renting hashrate
- Pool Mine HUSH via ASICs
- Pool Mine HUSH via renting hashrate
- Purchase on Centralized Exchange (dicey)

hush.is/yt - Mine directly to your own wallet

HushDEX

Decentralized Privacy Coin Exchange (DEX)

'What' ain't no country I ever heard of. Do they leak metadata in 'What'?



- Private Cross-Chain Swaps
- First pair: HUSH <> XMR
- Non-custodial
- Alices + Bobs
- Decentralized Application (dapp)

Coming Soon - trade.hush.is

How It's Going

Duke Leto 

@dukeleto

...

How It Started vs How It's Going

\$HUSH

Official Website: hush.is

YouTube: hush.is/yt

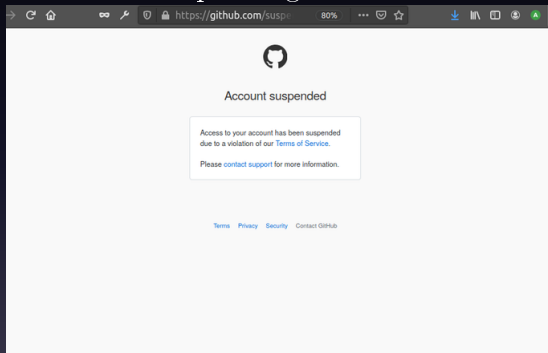
Telegram: hush.is/tg

Gitea: git.hush.is



Suspended From Github

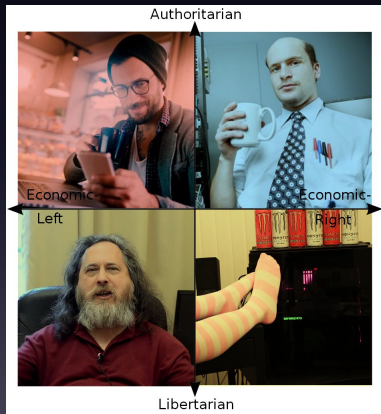
Stop Using Github



Github=Microsoft
A Censorship and Surveillance Platform

Join The Hush Community

Most types of Hackers and Cypherpunks welcome



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



Join The Hush Community



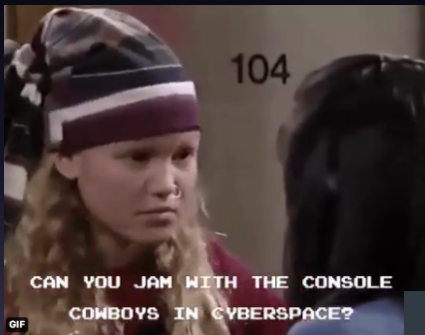
shoppinwithjoe.com

- Currently \$25 USD
- Limited Promotion:
- Show receipt → 5 HUSH
- 50000 HushChat encrypted messages

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



git.hush.is
In Zdust We Trust!
QED

