# What is Bitcoin Tumbling and why do it?

# Overview

The first Bitcoins were mined January 3rd 2009

nuary 12th the first transaction using the new currency took

Since then…

- Businesses now accept it for goods and services.
- Many other crypto-currencies have come into existence.
- An entire crypto-currency market has been created.
- For a short time one Bitcoin was on par with an ounce of gold.
- Some Greek citizens have used Bitcoin as a workaround to their countries capital controls.

# Bitcoin?

What is Bitcoin?

- It is a crypto-currency.
- Transactions are processed using the open source P2P system with the same name.
- A person or group going by Satoshi Nakamoto invited Bitcoin.
- It is the world’s first decentralized crypto-currency.
- Bitcoin transactions are stored on the blockchain

# Bitcoin?

How does one obtain Bitcoin?

- Bitcoins can be mined.
- They can be purchased.
- Goods or services can be exchanged for them.
- Someone can give them to you.

# Blockchain?

What is the Blockchain?

- A public ledger that records all Bitcoin transactions.
- Each block on the chain contains multiple transactions.
- The blockchain is decentralized and can be accessed by anyone.
- It is designed so that records are added but never deleted.

# Why Tumble?

Why would someone tumble Bitcoins?

- To increase their privacy.
- To remain anonymous.

# Bitcoin Tumbling?

What is Bitcoin Tumbling?

- An attempt to break the link between you and your Bitcoins.
- Exchange your Bitcoins with other people.
- These trades are not recorded on the Blockchain.
- The goal is to defeat Blockchain analysis.

# Bitcoin Tumbling?

How are Bitcoins Tumbled?

- Online Bitcoin Tumbling Service.
- Bitcoin Local Meetups and Exchanges.
- Purchasing another crypto-currency with Bitcoin then using those coins to purchase new Bitcoins.

# Why is Tumbling Needed?

- All Bitcoin Transactions are recorded publically to the Blockchain.
- Anyone can review these transactions at www.blockchain.info.

- Tumbling provides a layer of obfuscation.
- This extra layer is necessary for those who need to maintain their privacy and remain anonymous.
- This could help with the purchases or donations regarding issues that groups, societies or governments may not agree with.

# Can Tumbling be Dangerous?

Dangers! What Dangers?

- It is possible that your Bitcoins could be stolen by the tumbler administrator.
- The system could be hacked and result in the loss of your Bitcoins.

- Unwanted users could gain access to the tumbling logs.

# Bitcoin Tumbling Alternatives

Dashcoin?

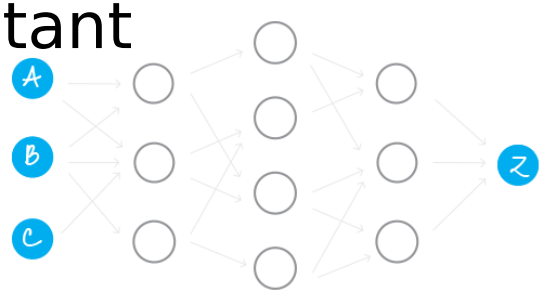
- Dashcoin is a privacy centric crypto-currency based on Bitcoin software
- Dashcoin was once called Darkcoin and Xcoin.
- The open source CryptoNote protocol provides added security.

One-time keys

Ring signatures

Blockchain Analysis Resistant

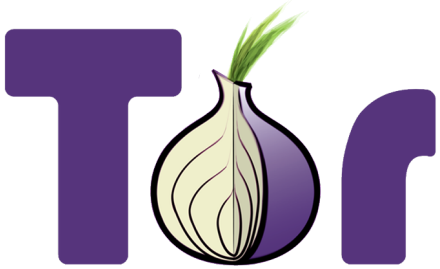
Untraceable trail

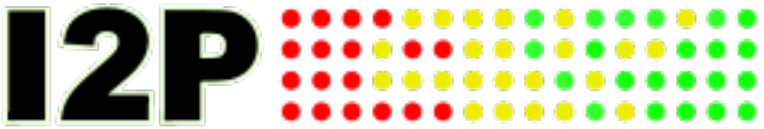



# Bitcoin Tumbling Alternatives

Anoncoin?

- Anoncoin is also a privacy centric crypto-currency based on the Bitcoin software. It is a fork of Litecoin.
- To gain privacy its transactions are routed through the TOR or I2P networks.





# Honerable Mentions

DarkWallet?

- Cooperative wallet feature.
- Stealth payments.
- CoinJoin mixing.
- **Still in alpha.**

# Honerable Mentions

Samourai?

- Supports Android only.
- Remote device wipe.
- Stealth Mode.
- **Still in alpha.**

# Final Thoughts

Once you've lost your privacy, you realize you've lost an extremely valuable thing.

Billy Graham