CoinJoin Privacy Technologies Explained

Author	josh
Date	2020-05-07 11:10:33

Overview

The Bitcoin blockchain is an incredible technology, in my opinion. It allows for totally decentralized, peer-to-peer transactions without trust thanks to a combination of interesting applied cryptography algorithms. However, Bitcoin lacks one very important property of money - fungibility. Individual coins are very traceable, and not indistinguishable in the way quarters or dollar bills are. Privacy matters for money, and there are technologies out there that help to solve this problem. One such technology is the broad concept known as *CoinJoin*.

Inputs, Outputs, and "Joining Coins"

A Traditional Transaction

In a normal Bitcoin transaction, the user's wallet creates one singular (and very traceable) transaction for their own business they are conducting. This transaction consists of inputs from the user's wallet, and creates new outputs for the receiver and for "change". If you're not quite familiar with UTXOs, consider readingthis previous tutorial that explains the concept in depth.

For example, let's say Bob wants to send Alice 0.5 BTC. Bob's wallet has a 1 BTC UTXO it must use up for this tx. So, the transaction creates one new output of 0.5 for Alice's address, and 0.5 back to Bob's wallet as "change". In this example, we're omitting miner fees for simplicity.

CoinJoin Transactions - Obfuscating Outputs

It's fairly obvious that with traditional transactions, blockchain analysis can show the flow of coins between addresses clearly over time and be used to identify parties participating in those transfers. However, *CoinJoin* transactions can be used to help obscure the flow of coins by pooling multiple user's transactions together and making coin flow much harder to track!

CoinJoins work by pooling user's transactions together and producing many outputs of *equal value*. For example, a CoinJoin finds many users that wish to make a transaction for 0.5 BTC, and combine them together in a single transaction. With many 0.5 BTC outputs and many inputs, it becomes infeasible to trace what "coins" where which, therefore enhancing the privacy of the users. This can be used to send transactions to a receiver, or "shuffle" the users own coins back to new addresses they own.

CoinJoin Concerns

There are a couple of important things to note about CoinJoins, and many more pieces that won't be covered in this article. It's not a perfect privacy tool, but can be extremely effective when used correctly.

First, it's best to avoid "change" in CoinJoin transactions - change UTXOs later spent can show that a user was involved in the initial CoinJoin transaction. It's best to consume an entire UTXO as a CoinJoin input. Second, the more users in a transaction, the better! This creates an "anonymity set" that's large enough that tracking users becomes impossible provided they use the technology correctly. 10 users in a CoinJoin is more secure than 3.

Finally, the broad idea of CoinJoin does *not* solve the problem of finding other users to join *with* in a way that is trustless. Other algorithms must be combined with CoinJoin technology to make it work well.

Implementations

As I mentioned, CoinJoin itself doesn't solve the problem of finding other users on the network to do joins with. So there are a variety of implementations that solve this problems in different ways, ideally in ways that are decentralized and trustless.

The first (not good) type of CoinJoin implementation is a centralized service. These are known as "mixers". These SHOULD NOT BE USED! Some mixers are scams that will steal your coins outright, and others are tracked so that coins that come out of them are "blacklisted" by exchanges and other services. This implementation relies on trust, which defeats the purpose of using cryptocurrencies in the first place!

Now, for good trustless technologies! It largely depends on the chain you wish to use. Bitcoin BTC has the well-regarded Wasabi wallet, which uses the ZeroLink protocol for trustless CoinJoins. Bitcoin Cash BCH uses it's own completely decentralized algorithm called CashShuffle, which is integrated into some wallets. Litecoin LTC has a community working on a protocol called MimbleWimble, which also implements a type of CoinJoin.

Privacy Protection - Join Those Coins!

Privacy protection is an important part of life and money. While Bitcoin, Bitcoin Cash, and Litecoin may be pseudonymous, they are not anonymous or privacy preserving in their raw form. By adding technologies like CoinJoin, these currencies can be used in a way that protects user privacy. This technology uses the UTXO blockchain design to combine user inputs and outputs into a singular transaction with many equal outputs, therefore obscuring the flow of coins between addresses. When used correctly, CoinJoins help users protect their privacy and make these coins fungible, an important property for a cash system to have.