Wrong Address Woes - What Happens if You Send BCH to a BTC address (and vice versa)

Author	josh
Date	2019-04-02 23:40:03

Overview

In the early days of the Bitcoin Cash hard fork, several users encountered a very serious problem with their transactions. In what might be a simple misreading of an address or confusion over the distinction between these two currencies, users were sending their funds to addresses *on the wrong blockchain*.

Users found out that this was a simple mistake to make. Bitcoin and Bitcoin Cash share the same address space - so an address that's valid on one is also valid on the other. And at the time, there was no formatting distinction between the two either. So all it took was accidentally copying an address that someone intended to be user for BTC, and suddenly a user was sending their BCH into the void (or so it seemed). The reverse could be true as well, with BTC (Bitcoin) being sent to an address intended to be used for Bitcoin Cash.

Let's take a look a what actually happens when this mistake is made, and what some solutions to the problem are.

A Deeper Look at BTC/BCH Addresses

The Address Space and Private Keys

When looking at this problem, it is important to understand why Bitcoin and Bitcoin Cash addresses were easily confused, and why this problem would occur in the first place.

Bitcoin addresses are derived from 256 bit private keys using elliptic curve cryptography, coupled with some extra steps that make addresses easy to verify and encoding that makes them easier to deal with. When a Bitcoin address is generated, a random 256 bit number is generated. The public key is then derived using an elliptic curve algorithm (specifically secp256k1). The public key is hashed twice, once with SHA256 and then once with RIPEMD160. Finally, a version prefix and checksum are added and the whole address is encoded in base58.

Both Bitcoin and Bitcoin Cash used the exact same mechanism for generating addresses from the same exact pool of private keys. This offers up some good news with regards to dealing with this problem!

Cross-Chain Address Ownership

So if the mechanism for generating addresses is the same in BCH and BTC, then that means that the owner of a BTC address is also the owner of the exact same address on the BCH chain! The

private key that the address was generated from proves ownership of the coins, and so the owner of the address will own coins sent to that address on either chain.

"Cross-Chain" Transaction Scenarios and Solutions

User sends BCH funds to their own BTC address

Let's take a closer look at what happens when a user accidentally sends Bitcoin Cash to their own Bitcoin address. It is common for users to send their own funds between different wallets, like purchasing on an exchange with a custodial system and sending funds to a wallet where they control the private keys.

When the user broadcasts this transaction, it is processed entirely by the *Bitcoin Cash* network. Even though this user's address came from their *Bitcoin (BTC)* wallet, nothing happens on the Bitcoin chain because these are two *entirely different* systems.

However, the BCH had to go somewhere! It may seem that it has been lost, but in reality it is now owned by the user's address *on the Bitcoin Cash blockchain*.

It is likely that our friend is panicking because they don't see the funds showing up in their Bitcoin Cash (BCH) wallet like they intended. However, they *do own the money* and just need to claim it!

Since the address spaces are the same between chains, our user *has the private key that controls this Bitcoin Cash.* All they need to do is export the private key from their Bitcoin wallet and import it into their Bitcoin Cash wallet, and the wallet will now recognize the funds as part of their BCH balance.

Further Complications

Thankfully in this situation, the mistake is a simple fix. The user controls the private key for the address they mistakenly sent their funds to, and so they have retained control of the funds the entire time. However, if a user sends funds to *someone else's* BTC address, they will have to explain this process to the (hopefully known) recipient and hope they will be generous enough to send the BCH funds back to our friend. If the owner of the address cannot be contacted in the real world, our friend is entirely out of luck.

The activation of segwit (segregated witness) on the Bitcoin (BTC) network further complicates things. The above process only holds true for simple P2PKH transactions. If Bitcoin Cash is sent to a Segwit BTC address, the funds cannot be recovered on the BCH blockchain because these address types are not supported on the network

The *CashAddr* Format

Thankfully, the developers in the Bitcoin Cash ecosystem have created a new address format unique to BCH that is easily distinguishable from legacy Bitcoin addresses. A base58check encoded BTC address (non-segwit) looks like this:

`1LxWuAJLENgSpQic736V3ZxmRVJp44uGZV`

Whereas a base32 CashAddr BCH address looks like this:

`qrnzx44wf8swjl2v9c36jcmch7a4yefkav0z4rxm8g`

It is now much harder to make the same mistakes when dealing with addresses thanks to this format

Wrong Address? Not All Hope Is Lost!

Once we understand that Bitcoin and Bitcoin Cash share the same address space (and therefore private key space), it is a bit less scary to deal with this problem of "cross-chain" transactions. No transaction is really cross chain, it is simply sent to the mistaken address on the chain you sent it from. So, if you control the private keys for an address on one chain, you can easily claim funds you mistakenly sent to that address on the other. If you send BCH to your BTC address, you simply need to import that private key in your BCH wallet to claim the funds.

There are complications due to segwit and further problems for addresses our user doesn't own. These are a reminder to always exercise caution when creating cryptocurrency transactions, as mistakes are often costly and irreversible. However, new formats like CashAddr have made these mistakes harder to make, so hopefully you never have a need to recover funds in the first place!