Recovering BCH (Sent to BTC Address)

Author	josh
Date	2019-12-23 21:00:01

Overview

Many of the viewers of my tutorial on what happens when you send BCH to a BTC address have asked for more specific help on how to recover funds in this scenario. Fortunately, not all is lost if this happens - it just depends on the context. For non-custodial wallets (where the user controls the private key), it's fairly straightforward to recover the lost BCH and send it back to a wallet the user would like to use. It is important to note, however, that this only works with these non-custodial wallets. If a user sends funds to a custodial wallet (like CashApp or an exchange), they'll have to get in touch with that exchange's customer service for help.

BCH Fund Recovery

What Actually Happens...

If a user sends BCH to a "BTC" address, the funds never really leave the Bitcoin Cash blockchain. The confusion happens because BCH and BTC legacy addresses are backward compatible - so when the user creates the BCH transaction with the BTC wallet address as the receiver, the transaction is totally valid and is sent.

But, the BTC and BCH addresses also share the *same private key*. Therefore, if the user has access to the BTC wallet's *recovery phrase* (or the private key directly), they can import/sweep that key into a BCH wallet to get the funds back.

An Example Scenario, With Recovery Steps

For this tutorial, I "accidentally" sent some Bitcoin Cash to a Bitcoin address provided by a blockchain.info wallet. The funds do not show up in my BTC balance, because I actually did this on the BCH chain.

Looking at a block explorer, we can see the mistaken address for this transaction. In legacy format (BCH/BTC backward compatible), we see the address is `1Ka4YZ19kq87yXUAPXMt9KZLd2eap1pT4Y`

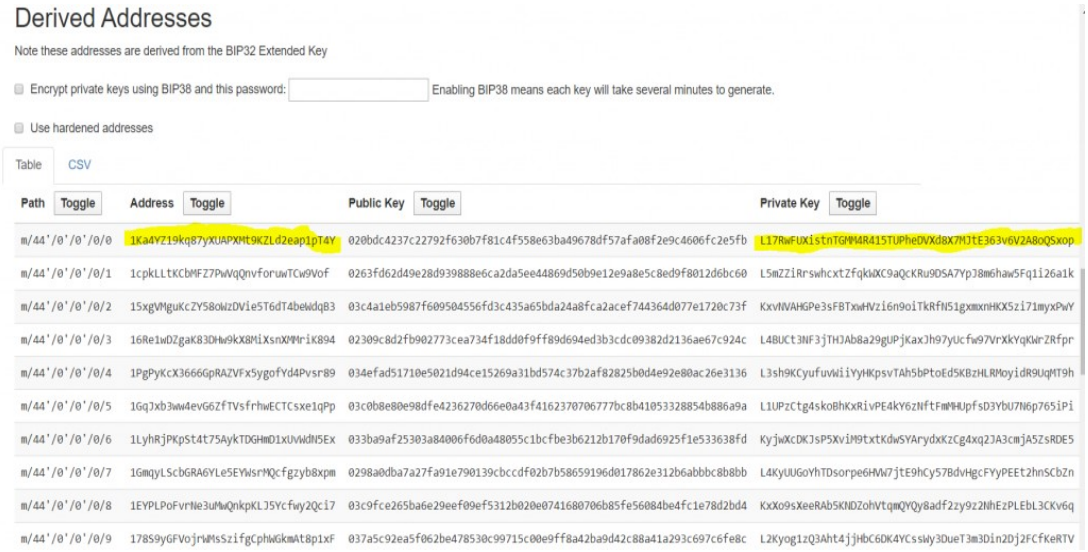
Now what we need to do is to get the associated *private key* for this address. In this case, blockchain.info provides a mnemonic *seed phrase* used to generate all the wallet's private keys and associated addresses. Therefore, if we get this seed phrase we can extract the specific key for this address and import it into another wallet we control. The seed phrase for our test wallet here is:

```
water pulse panel anchor impulse brown effort cake open drastic bright aerobic
```

It's important that you don't reuse this seed phrase for any of your own wallets - anyone who's seen this tutorial could steal your money!

Now what we can do is import this seed phrase into a mnemonic tool. I'm a big fan of [Ian Coleman's Bip39 Mnemonic Code tool.](#) An important note - if you're doing this with real funds, download the webpage and run the tool when your PC is *offline*. Ian's tool is trusted in the community, but it's best practice to never but private information like seed phrases into online tools - your funds could be stolen by a nefarious website.

When the seed is put in the tool, the derived addresses and keys will be shown in a table like this:



Derived Addresses

Note these addresses are derived from the BIP32 Extended Key

Encrypt private keys using BIP38 and this password: Enabling BIP38 means each key will take several minutes to generate.

Use hardened addresses

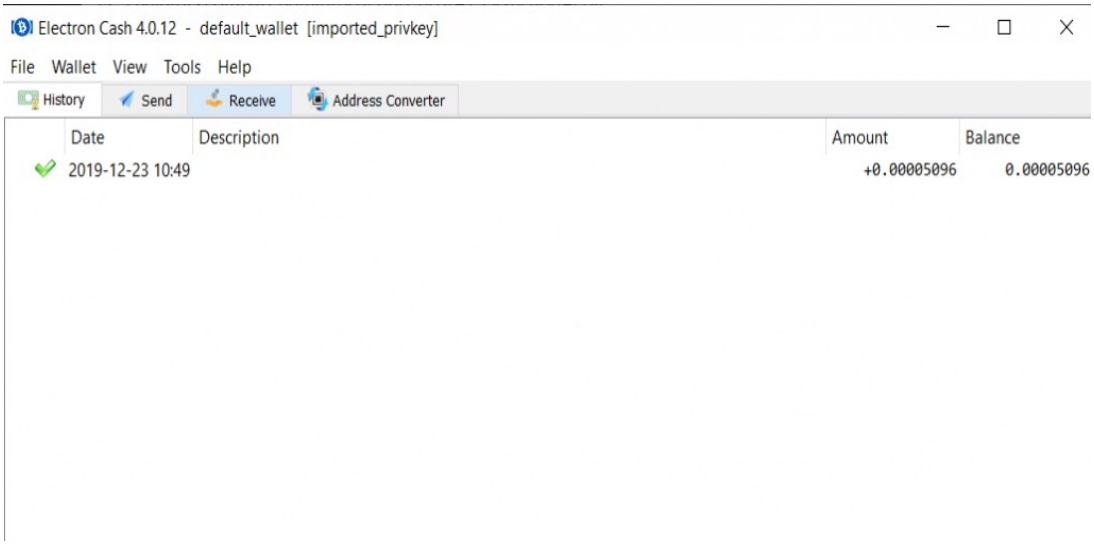
Table CSV

Path Toggle	Address Toggle	Public Key Toggle	Private Key Toggle
m/44'/0'/0'/0/0	1Ka4YZ19kq87yXUAPXHt9KZLd2eap1pT4Y	020bdc4237c22792f630b7f81c4f558e63ba49678df57afa08f2e9c4606fc2e5fb	L17RwFUXistnTGMM4R415TUPheDVXd8X7MJtE363v6V2A8oQSxop
m/44'/0'/0'/0/1	1cpkLLtKCbMFZ7PwVqQnvforuwTCw9Vof	0263fd62d49e28d939888e6ca2da5ee44869d50b9e12e9a8e5c8ed9f8012d6bc60	L5mZZiRrswhcxtZfqkWXC9aQcKRu9DSA7YpJ8m6haw5Fq1i26a1k
m/44'/0'/0'/0/2	15xgVMguKcZY58oWzDVie5T6dT4beWdqB3	03c4a1eb5987f609504556fd3c435a65bda24a8fca2acef744364d077e1720c73f	KxvNVAHGPe3sFBTxwHVzi6n9oiTkRfN51gxmxnHKX5zi71myxPwY
m/44'/0'/0'/0/3	16Re1wDZgaK83DHw9kX8MiXsnXMMriK894	02309c8d2fb902773cea734f18dd0f9ff89d694ed3b3cdc09382d2136ae67c924c	L4BUCt3NF3jTHJAbBa29gUPjKaxJh97yUcfw97VrXkYqKWrZRfpr
m/44'/0'/0'/0/4	1PgPyKcX3666GpRAZVFx5ygofYd4Pvsr89	034efad51710e5021d94ce15269a31bd574c37b2af82825b0d4e92e80ac26e3136	L3sh9KCyufuvWiiYyHKpsvTAh5bPtoEd5KBzHLRMoyidR9UqMT9h
m/44'/0'/0'/0/5	1GqJxb3ww4evG6ZfTVsfrhwECTCsxe1qPp	03c0b8e80e98dfe4236270d66e0a43f4162370706777bc8b41053328854b886a9a	L1UPzCtg4skoBhKxRivPE4kY6zNftFmM4UpfsD3YbU7N6p765iPi
m/44'/0'/0'/0/6	1LyhRjPKpSt4t75AykTDGHmD1xUvWdN5Ex	033ba9af25303a84006f6d0a48055c1bcfbe3b6212b170f9dad6925f1e533638fd	KyjwXcDKJsP5XviM9txtKdwSYArydxKzCg4xq2JA3cmjA5ZsRDE5
m/44'/0'/0'/0/7	1GmqyLScbGRA6YLe5EYWsrMQcfgzyb8xpm	0298a0dba7a27fa91e790139cbccdf02b7b58659196d017862e312b6abbbc8b8bb	L4KyUUGoYhTDsorpe6HVW7jtE9hCy57BdvHgcFYyPEEt2hnSCbZn
m/44'/0'/0'/0/8	1EYPLPoFvrNe3uMwQnkpKLJ5YcfWy2Qci7	03c9fce265ba6e29eef09ef5312b020e074168070 6b85fe56084be4fc1e78d2bd4	KxXo9sXeeRAb5KNDZohVtqmQYQy8adf2zy9z2NhEzPLEbL3CKv6q
m/44'/0'/0'/0/9	178S9yGFVojrWMsSzifgCphWGkmAt8p1xF	037a5c92ea5f062be478530c99715c00e9ff8a42ba9d42c88a41a293c697c6fe8c	L2KyogizQ3Aht4jjHbC6DK4YCssWy3DueT3m3Din2Dj2FCfKeRTV

Search for the address you mistakenly sent the funds to. If you've used your wallet a lot, you may have to generate more child addresses. Also, if you don't see the address here, don't panic - play around with some derivation settings. Different wallets use different paths and that sort of thing, but in this case our wallet used the defaults.

Now you need to copy the Wallet Import Format *private key* shown next to the address - this will allow you to unlock the funds. What we'll do here is *import or sweep* the address into a BCH wallet we control to recover the funds. Note the distinction - an *import* keeps the funds in the same address. If you add this to a wallet with an existing backup phrase, the imported address *will not be protected* by that backup phrase. *Sweeping* is better - this will create a new transaction that sends the recovered funds to a new address controlled by the wallet's phrase.

Your funds are back! For this sample recover, I imported the funds into an Electron Cash wallet on desktop.



Fund Recovery - It's All About Keys

The most critical step in recovering lost funds is understanding that whoever *controls the private keys* owns the lost funds. If you've sent your funds off to an exchange or app like CashApp, you'll need help from them because you don't control the keys. But if you accidentally sent funds to an address provided by your own BTC wallet, you can follow these steps to get your BCH back into your normal BCH wallet. It's a matter of getting the key for the mistaken address into a BCH wallet that recognizes the funds on the blockchain.

I hope this helps! It can be scary to lose funds in the cryptocurrency space, where things are a lot more final than in the world of banking. Ultimately though, cryptocurrency gives us more control over our own money and that's a great thing.

Oh and as a little easter egg for my viewers - I left the BCH for this tutorial in the sample address. If you want it, it's yours :) First recovered, first served.