Understanding Address Balances for UTXO Blockchains

Author	josh
Date	2019-03-05 18:00:32

Overview

When you open your Bitcoin, Bitcoin Cash, or Litecoin wallet, you'll see a balance just like you do when you open your bank app. At the end of the day, you just want to know how much currency you own, right? You may be curious, however, how your total balance is calculated in the world of cryptocurrencies. With your local bank, a centralized authority (the bank itself) keeps track of the state of your account as one unit. The bank tracks deposits and withdrawals, and keeps a running tally of your available balance for you. The Bitcoin blockchain, however, does things a little differently. This blockchain (and the BCH and LTC blockchains, to name a few others) use a concept called the UTXO to deal with available balances. If that sounds completely foreign, don't fret. It turns out UTXO-based chains function quite like the physical cash in your wallet!

UTXOs explained

What is a UTXO?

An *unspent transaction output*, commonly referred to as a *UTXO* is a chunk of cryptocurrency that is owned by a user's wallet and available for the user to spend. More specifically, a UTXO is owned by a particular address in the user's wallet, and therefore the associated private key. A raw UTXO looks something like this when pulled from a block explorer API: `{ "txid": "2e2a921b819c261822dfa0931523a54b0c8900182c20d4be25ff333982a8f76a", "amount": 0.10401187, "confirmations": 306 }` This UTXO is pulled from the bitcoin.com REST API, with some bits of data removed for simplification. If you want to try querying this yourself, you can opening this API call in your browser.

Deciphering UTXO data

Now let's look a little closer at this UTXO. The first data field that we see is the txid, which is a long string of data that looks meaningless. This data is the hash of the transaction that created this UTXO. In other words, this particular transaction *sent money to this address*. The second item is fairly self explanatory: this is the Bitcoin amount sent to the address in this UTXO. Finally, the number of confirmations indicates how many times a new block has been added on top of the block containing this transaction. The more confirmations, the more "sure" we can be that this transaction is a permanent part of blockchain history and owned by the address.

How do UTXO's function?

UTXOs function in a way that is remarkably similar to physical cash. *Think of a UTXO like a five dollar bill in your wallet*. A UTXO is a bill available for you to spend in a future Bitcoin

transaction. Let's say your grandma sent you $5 in a card for Christmas. You now have $5 in your wallet ready to use when you go to the store. Much like dollar bills, UTXOs *must be spent entirely* in a new transaction. If you go to the store to buy a bag of chips and a drink for $2.50, you cannot tear the $5 bill in half and give it to the cashier, can you? You give the person the entire bill, and get $2.50 back in change. Bitcoin UTXOs function in the exact same way in a transaction. If you have a UTXO your address owns for 0.1 Bitcoin and you want to send your friend 0.05 Bitcoin, your wallet will create a transaction that sends their address 0.05 BTC in a new UTXO, and sends 0.05 back to your address in change!

UTXO's and Your Wallet Balance

Now that we understand how UTXOs work, understanding how your wallet tracks your balance is pretty straightforward! Your wallet contains a bunch of private keys and a bunch of addresses derived from those keys. Each address can have a bunch of UTXOs associated with that address, and your wallet balance is the *sum total* of all those UTXOs. It's that simple. Just like you may have some 1's, 5's, and 20's in your physical wallet, your Bitcoin wallet can have a bunch of UTXOs in any denomination of Bitcoin. When you go to send Bitcoin to another user, your wallet bundles up as many UTXOs as it needs to create a transaction in that amount and uses them as "inputs" for that transaction. Unlike physical cash, however, your wallet can turn your $5 and $10 UTXOs in to a fresh $20 bill.

What's in your (Bitcoin) wallet? UTXOs of course!

Again, UTXOs are the dollar bills of the Bitcoin world. Blockchains based on this model include popular digital currencies such as Bitcoin Core, Bitcoin Cash, and Litecoin. Other popular currencies such as Ethereum use an account based model that functions more like a traditional bank account, tracking inputs, outputs, and balances as state changes over time. The good news is, understanding the slightly more complex UTXO model is fairly trivial with a good analogy, and this model functions like the cash we use every day. If you have a Bitcoin Cash address, you can try viewing your UTXO "dollar bills" yourself using a project I created for this purpose. This project features an API that digests raw blockchain data and outputs an easy to understand format so you can learn these concepts. On top of the API, there's a nice and simple React frontend that formats the data in a table. The code is available on Github, and if you visit https://jmcintyre.net/sites/myaddrbal_client/ you can try it for yourself! Here's an example with one of my BCH addresses used above:

Happy crypto learning!