Digital Dollar Bills: Understanding UTXOs and Change

Author	josh
Date	2020-04-22 17:19:25

Overview

Have you ever looked at a transaction on a Bitcoin block explorer, and were confused by all the different amounts shown? Wondered what these "inputs" and "outputs" listed in the transaction mean? Bitcoin and other cryptocurrency transactions may seem similar in some ways to other digital payment mechanisms like debit cards or PayPal, but their underlying structure is actually much more similar to the way we use cash. Let's discuss the basics of UTXOs and change in transactions.

UTXOS, Inputs, Outputs, and Change

What is a UTXO?

When you look at your cryptocurrency wallet balance, what are you actually seeing? Many of the most popular blockchains use a *UTXO* model for tracking address balances, much different than the "account" model we are used to when dealing with our bank accounts. Instead of dealing in "deposits" and "withdrawals", these blockchains track *Unspent Transaction Outputs*, abbreviated as UTXOs.

A UTXO is like a digital dollar bill, owned by a receiving address. When someone sends you Bitcoin, Litecoin, Bitcoin Cash, or DigiByte, the transaction creates a new UTXO in that amount that is owned by your receiving address. The UTXO is "locked" by the private key associated with your address, and therefore can only be spent in a future transaction by you!

Inputs and Outputs

So how are UTXOs used in transactions? When you go to spend some amount of cryptocurrency, your wallet creates a transaction using UTXOs that your wallet addresses owned as *inputs* to that transaction. Your wallet signs the transaction using your private keys, which tells other users of that currency that you are the rightful owner of those funds.

These inputs are said to be "consumed" by the transaction, and new outputs are created that are associated with the receiver's address. As new transactions are created, there's a perpetual cycle on the blockchain of consuming UTXO inputs and creating UTXO outputs!

Understanding Change

An important to understand property of UTXOs is that they cannot be "split", much like US dollar bills cannot be "split" in a cash transaction. If you buy an item that costs $15 dollars, you may hand the cashier a $20 bill. You can't rip off 1/4 of the 20 though, it doesn't work that way! Rather, the cashier will hand you back $5 in "change" to complete the transaction.

UTXO blockchains behave the same exact way! If you have a 1 bitcoin UTXO in your wallet and want to make a 0.5 bitcoin purchase, your wallet will "consume" that 1 BTC UTXO in the transaction, and create *two* new outputs. One UTXO for 0.5 BTC goes to the *receiver*, and is owned by their address. The other 0.5 BTC goes back into your wallet into a *change address*, which is simply another address your private keys/seed phrase control.

Let's look at a concrete example of this. DigiByte is another example of a UTXO blockchain. This transaction with hash f1745f8a1d52b781f0ff910a32eb6bf5682d2b04ed26c23466c425f479405c42 consumes a UTXO worth 3703.49823286 DigiByte, but the receiver is only getting .0001. The wallet owner receives 3703.49821286 back as change, and a small fee goes to the miner. It's important to know that miner fees are *not* denoted as an additional UTXO, but rather as the difference between the sum of all outputs and the sum of all inputs.

UTXOs - Like Digital Dollar Bills

UTXO blockchains behave in a way that is remarkably similar to cash transactions. When you receive cryptocurrency, you receive it as a UTXO "bill" for some amount. When you go to spend that later, you must use that whole "bill" for the transaction, and receive any difference back as "change" in the form of a new UTXO. Many of the most popular blockchains such as Bitcoin, Bitcoin Cash, Litecoin, and DigiByte use this model. The most notable outlier is Ethereum, which uses an account model that tracks balance state with deposits and withdrawals.

So next time you create a transaction with one of these cryptos, try viewing the transaction in a block explorer and seeing its construction. Note the inputs and outputs, and see if you can decipher which are for the receiver, which are change, and how the miner fees are calculated. It's great to understand how this technology works under the surface!