The Waiting Game: The Mempool and Transaction Fees

Author	josh
Date	2020-03-19 18:58:18

Overview

Have you ever sent a Bitcoin transaction, only to panic and realize the money hasn't shown up in the receiver's wallet? Maybe you were sending from a mobile phone wallet to a hardware wallet or exchange, and became afraid that your money was lost! Don't fret, you didn't lose any money at all. Your transaction is simply stuck somewhere called the *mempool*, waiting for the confirmation. Let's discuss what the mempool is, and how protocol rules effect transaction fees and confirmation times.

The Life of a Transaction

How do Transactions Get Processed?

In order to understand some of the issues surrounding transactions, let's first understand how they are actually processed. When you use your cryptocurrency wallet to create a transaction (send money to another wallet), your wallet *signs* and *broadcasts* that transaction out to the network.

Your transaction is flooded out to all of the nodes (including miners) on that network. But they don't immediately accept the transaction as valid, it must first be included in a *block* produced by a miner. You can think of a block as a "batch processing" of transactions. So, when a transaction is waiting to be included in the block, it is included in a data structure called the *mempool*. Each node constructs its own mempool based on the transactions it receives from other nodes, but for the most part each nodes mempool will have roughly the same set of unconfirmed transfers.

The Mempool and Block Construction

From this mempool, mining nodes put together a potential block of "batch processed" transactions while they work on the network's *proof-of-work* problem that will finalize the block. The miner that solves this problem gets rewarded with new coins, as well as all the transaction fees from this block.

But before we can understand fees, we need to understand the constraints networks put on the processing of new blocks. First, blocks often have *size limits*. Bitcoin limits the size of a block to 4 *weight units*, a special calculation based on segregated witness rules. Historically, this limit was 1 megabyte, referring to the actual size of the transaction data. Many still (somewhat erroneously) refer to Bitcoin's block size limit this way.

There's also a rough *block time*. Bitcoin's proof-of-work problem is adjusted so that new blocks are processed roughly every 10 minutes. Most Bitcoin forks such as Bitcoin Cash and Bitcoin SV follow this same time constraint.

Constraints' Effect on Fees

Now that we understand the limits on transaction processing, it's fairly intuitive to understand the *fee market* that emerges. On some networks like Bitcoin, there are more transactions in the mempool than can be processed in one block! That means we have a supply and demand problem!

If there is more transactions than can be processed in one block, miners will construct a block with the *highest fee* transactions - since that means they get the highest reward. Therefore, the more transactions are waiting in the mempool (a backlog), the higher fees will be on the network on average. Most user's don't want to wait, so they will pay a higher fee to have their transaction processed quickly.

Now, this is not the case for every network. There are ways to adjust these constraints so the mempool is *usually* cleared with every block. Some networks, such as Litecoin, use a faster *block time*. LTC processes blocks roughly every 2.5 minutes. Since blocks are processed faster, the mempool clears out faster. Some other networks, such as Bitcoin Cash, have a higher *block size* limit. BCH will process blocks much larger than 1MB, meaning that the mempool is always cleared out every 10 minutes.

With these adjustments, networks aim to keep fees very low with some tradeoffs. Some Bitcoin experts claim that these limits prevent centralization and keep full nodes affordable, while others (including myself) disagree with this premise. As well, faster block times can cause problems with "orphaned blocks", blocks that are valid but are not included in the chain due to network lag (another miner solves the same block, which gets accepted first and propagated in a "race" scenario).

Transaction Troubles? Don't Worry!

Now that we understand the mempool and transaction fees, you can see that a long-outstanding transaction does *not* mean you lost funds! It simply means your fee was too low for a clogged-up network. You will have to wait, but your money is not lost. If it takes a very long time for the network to clear, your transaction may be dropped from the mempool entirely. In that case, your funds are safely back in your wallet. Alternatively, some Bitcoin wallets also allow something called "Replace by Fee", where you can rebroadcast a transaction with a higher fee to help speed things up. And finally, if you want fast transactions and low fees all the time, another cryptocurrency may fit your use cases better. Bitcoin Cash, Litecoin, and DigiByte are some currencies that I use for fast, low fees transfers. It's up to you and your needs!