Mempool Replacements

Current Replace-by-Fee Policy

A transaction conflicts with an in-mempool transaction ("directly conflicting transaction") if they spend one or more of the same inputs. A transaction may conflict with multiple in-mempool transactions.

A transaction ("replacement transaction") may replace its directly conflicting transactions and their in-mempool descendants (together, "original transactions") if, in addition to passing all other consensus and policy rules, each of the following conditions are met:

1. The directly conflicting transactions all signal replaceability explicitly. A transaction is signaling replaceability if any of its inputs have an nSequence number less than (0xffffffff - 1).

   Rationale: See BIP125 explanation.

2. The replacement transaction only include an unconfirmed input if that input was included in one of the directly conflicting transactions. An unconfirmed input spends an output from a currently-unconfirmed transaction.

   Rationale: When RBF was originally implemented, the mempool did not keep track of ancestor feerates yet. This rule was suggested as a temporary restriction.

3. The replacement transaction pays an absolute fee of at least the sum paid by the original transactions.

   Rationale: Only requiring the replacement transaction to have a higher feerate could allow an attacker to bypass node minimum relay feerate requirements and cause the network to repeatedly relay slightly smaller replacement transactions without adding any more fees. Additionally, if any of the original transactions would be included in the next block assembled by an economically rational miner, a replacement policy allowing the replacement transaction to decrease the absolute fees in the next block would be incentive-incompatible.

4. The additional fees (difference between absolute fee paid by the replacement transaction and the sum paid by the original transactions) pays for the replacement transaction's bandwidth at or above the rate set by the node's incremental relay feerate. For example, if the incremental relay feerate is 1 satoshi/vB and the replacement transaction is 500 virtual bytes total, then the replacement pays a fee at least 500 satoshis higher than the sum of the original transactions.

   Rationale: Try to prevent DoS attacks where an attacker causes the network to repeatedly relay transactions each paying a tiny additional amount in fees, e.g. just 1 satoshi.

5. The number of original transactions does not exceed 100. More precisely, the sum of all directly conflicting transactions' descendant counts (number of transactions inclusive of itself and its descendants) must not exceed 100; it is possible that this overestimates the true number of original transactions.

   Rationale: Try to prevent DoS attacks where an attacker is able to easily occupy and flush out significant portions of the node's mempool using replacements with multiple directly conflicting transactions, each with large descendant sets.

This set of rules is similar but distinct from BIP125.

History

- Opt-in full replace-by-fee (without inherited signaling) honoured in mempool and mining as of **v0.12.0** (PR 6871).
- BIP125 defined based on Bitcoin Core implementation.
- The incremental relay feerate used to calculate the required additional fees is distinct from `minRelayTxFee` and configurable using `-incrementalrelayfee` (PR #9380).
- RBF enabled by default in the wallet GUI as of **v0.18.1** (PR #11605).