Dash InstantSend Overview

InstantSend is a feature provided by the Dash network that allows for zero-confirmation transactions to be safely accepted and re-spent. The network attempts to lock the inputs of every valid transaction when it is broadcast to the network. Every secured transaction is included in a following block in accordance with standard blockchain principles.

InstantSend is enabled by the Masternode Network which comprises approximately 5,000 masternode servers. These nodes are differentiated from standard nodes by having proven ownership of 1,000 Dash, making the network highly resistant to Sybil attacks. Masternodes form Long-Living Masternode Quorums (LLMQs), which are responsible for providing near instant certainty to the transaction participants that the transaction inputs cannot be respent, and that the transaction will be included in a following block instead of a conflicting transaction.

This concept works as an extension to Nakamoto Consensus. InstantSend enables transacted funds to be immediately and securely respent by the recipient, even before the transaction is included in a block.

Receiving InstantSend Transactions

Receiving an InstantSend Transaction introduces two requirements:

1. The ability to determine the “InstantSend Status” of a given transaction.
2. The ability to adjust “Confirmation Status” independently of block confirmation.

InstantSend Status is typically determined through direct connection with the dash daemon, ZMQ notification, or through the usage of an external wallet notification script.

Direct Connection: InstantSend Status can be identified through direct connection with the Dash daemon using JSON-RPC protocol. The “instantlock” attribute of the JSON response reflects the status of the transaction and is included in the following commands:

getrawmempool, getmempoolancestors, getmempooldescendants, getmempoolentry, getrawtransaction, decoderawtransaction, gettransaction, listtransactions, listsinceblock.

ZMQ Notification: Whenever a transaction enters the mempool and whenever a transaction is locked in the mempool, ZMQ notifications can be broadcast by the node. A list of possible ZMQ notifications can be found here.

The following notifications are relevant for recognizing transactions and their corresponding instantlocks:

```
zmqpubhashtx, zmqpubhashtxlock, zmqpubrawtx, zmqpubrawtxlock
```

Wallet Notification: The Dash Core Daemon can be configured to execute an external script whenever an InstantSend transaction relating to that wallet is observed. This is configured by adding the following line to the dash.conf file:

➔ instantsendnotify=/path/to/concurrent/safe/handler %s

This is typically used with a wallet that has been populated with “watch-only” addresses.

Broadcasting InstantSend Transactions

Since Dash v0.14.0 established LLMQs on the Dash network, quorums will now attempt to lock every valid transaction by default without any additional fee or action by the sending wallet or user. A transaction is eligible for InstantSend when each of its inputs

is considered confirmed. This is the case when at least one of the following circumstances is true:

- the previous transaction referred to by the input is confirmed with 6 blocks
- the previous transaction is confirmed through an older InstantSend lock
- the block containing the previous transaction is ChainLocked

When checking the previous transaction for an InstantSend lock, it is important to also do this on mempool (non-mined) transactions. This allows chained InstantSend locking.

Additional Resources

The following resources provide additional information about InstantSend and are intended to help provide a more complete understanding of the underlying technologies.

- InstantSend Technical Information
- InstantSend Developer Documentation
- DIP0010: LLMQ InstantSend
- Product Brief: Dash Core v0.14 Release