Shared Libraries

bitcoinconsensus

The purpose of this library is to make the verification functionality that is critical to Bitcoin's consensus available to other applications, e.g. to language bindings.

API

The interface is defined in the C header `bitcoinconsensus.h` located in `src/script/bitcoinconsensus.h`.

Version `bitcoinconsensus_version` returns an `unsigned int` with the API version *(currently `1`)*.

Script Validation `bitcoinconsensus_verify_script` returns an `int` with the status of the verification. It will be `1` if the input script correctly spends the previous output `scriptPubKey`.

Parameters

- `const unsigned char *scriptPubKey` - The previous output script that encumbers spending.
- `unsigned int scriptPubKeyLen` - The number of bytes for the `scriptPubKey`.
- `const unsigned char *txTo` - The transaction with the input that is spending the previous output.
- `unsigned int txToLen` - The number of bytes for the `txTo`.
- `unsigned int nIn` - The index of the input in `txTo` that spends the `scriptPubKey`.
- `unsigned int flags` - The script validation flags *(see below)*.
- `bitcoinconsensus_error* err` - Will have the error/success code for the operation *(see below)*.

Script Flags

- `bitcoinconsensus_SCRIPT_FLAGS_VERIFY_NONE`
- `bitcoinconsensus_SCRIPT_FLAGS_VERIFY_P2SH` - Evaluate P2SH (BIP16) subscripts
- `bitcoinconsensus_SCRIPT_FLAGS_VERIFY_DERSIG` - Enforce strict DER (BIP66) compliance
- `bitcoinconsensus_SCRIPT_FLAGS_VERIFY_NULLDUMMY` - Enforce NULLDUMMY (BIP147)
- `bitcoinconsensus_SCRIPT_FLAGS_VERIFY_CHECKLOCKTIMEVERIFY` - Enable CHECKLOCKTIMEVERIFY (BIP65)
- `bitcoinconsensus_SCRIPT_FLAGS_VERIFY_CHECKSEQUENCEVERIFY` - Enable CHECKSEQUENCEVERIFY (BIP112)

- `bitcoinconsensus_SCRIPT_FLAGS_VERIFY_WITNESS` - Enable WITNESS (BIP141)

Errors

- `bitcoinconsensus_ERR_OK` - No errors with input parameters *(see the return value of* ***`bitcoinconsensus_verify_script`*** *for the verification status)*
- `bitcoinconsensus_ERR_TX_INDEX` - An invalid index for `txTo`
- `bitcoinconsensus_ERR_TX_SIZE_MISMATCH` - `txToLen` did not match with the size of `txTo`
- `bitcoinconsensus_ERR_DESERIALIZE` - An error deserializing `txTo`
- `bitcoinconsensus_ERR_AMOUNT_REQUIRED` - Input amount is required if WITNESS is used
- `bitcoinconsensus_ERR_INVALID_FLAGS` - Script verification `flags` are invalid (i.e. not part of the libconsensus interface)

Example Implementations

- NBitcoin (.NET Bindings)
- node-libbitcoinconsensus (Node.js Bindings)
- java-libbitcoinconsensus (Java Bindings)
- bitcoinconsensus-php (PHP Bindings)