Code Review of NoLimitCoin-Core

Repository

https://github.com/NoLimitCoin/NoLimitCoin-Core.git

Overview

NoLimitCoin-Core (hereafter referred to as "NLC2") is most likely cloned directly from BitcoinDark[i] with a first commit on 9/3/2016[ii]. Other similar coins cloned from the BitcoinDark (hereafter referred to as "BTCD") repository are xcoin[iii] and CrocodileCash[iv]. BTCD has been a top 100 market cap coin according to CoinMarketCap[v] (#78 at the time of review), and has been listed at Bittrex, Poloniex, and Cryptopia. With a market cap of over $170 M, BTCD has made an attractive target for attackers. BTCD is therefore a very robust starting point. NLC2 stays very close to the BTCD codebase, deviating in ways that do not influence this robustness of the core code.

NLC2 Core Runtime Logic Changes

NLC2 makes limited **core** changes with respect to the BTCD codebase with the following minor exceptions:

- NLC2 adds functions to backup and restore blockchain data
  - `backupBlockchainData()`
  - `restoreBlockchainData()`
  - `copyDir()`
  - associated data structures for these operations: `blkIndexLocation`, `databaseLocation`, `txLevelDBLocation`, etc.
- NLC2 provides automated restoration of blockchain data (a.k.a. "restoring from a snapshot") upon failure to load the block index, executed during the application initialization (`AppInit2()`)
- NLC2 removes non-essential BTCD functions (`unstringify()` and `getstakers()`)
- NLC2 removes runtime logic and non-essential BTCD functions for creating a configuration template upon launch (`randomStrGen()` and `createConf()`)
- NLC2 removes a non-essential debugging check of proper `CTransaction` serialization in the RPC function `signrawtransaction()`
- NLC2 adds logic to split a single sending transaction to self into an arbitrary number of equal, smaller transactions using the parameter `nSplitBlock` in `CWallet::CreateTransaction()`
- NLC2 adds logic to automatically return change to one of the input destinations using a boolean coin control flag in `CWallet::CreateTransaction()`
- NLC2 adds the method `CWallet::GetStakeWeightFromValue()` that calculates the stake weight from age and value – this method is not used in the core (daemon) but in the Qt

NLC2 Core Parameter Changes

NLC2 includes the following parameter changes needed for security and smooth operation:

- Alert public keys are unique (`pszMainKey`, `pszTestKey`)
- Checkpoint public key is unique (`CSyncCheckpoint::strMasterPubKey`)
- The four byte `pchMessageStart` that leads peer-to-peer messages is unique
- The peer-to-peer port number is unique
- The `LAST_POW_BLOCK` is consistent with desired emission

NLC2 Core Concerns

Potential concerns in the NLC2 core code have no impact, but should be mentioned for completeness.

NLC2 has values for the following constants related to genesis that generally would be flagged in a review, but are of no consequence given that (1) distribution was by coin sale and (2) the current codebase represents a coin swap.

- `pszTimeStamp` is unique, but does not reference an historical event
- The genesis block `nTime` and `vtx[0].nTime` (`CTransaction`) is about three months before the first commit

Other Notes

All three seed nodes point to IP addresses of functional peers (`strDNSSeed[]`).

NLC2 Qt GUI Changes

NLC2 makes the following changes to the Qt client

- NLC2 adds a built-in block browser
- The NLC2 coin control dialog includes stake weight utilizing the new method `CWallet::GetStakeWeightFromValue()`
- NLC2 adds a launch at login controller for OS X
- NLC2 adds some standard code changes related to notifications, for compilation on newer versions of OS X
- NLC2 adds GUI control elements and logic to split transactions to self and to automatically return change to one of the input destinations

---

i BitcoinDark: https://github.com/laowais/bitcoindark.git
ii https://github.com/NoLimitCoin/NoLimitCoin-Core/commit/75d6e22a00eae30e4c7923fe3c1079e288390aa8
iii https://github.com/jimblasko/xcoin.git
iv https://github.com/RangaBoom/CrocodileCash.git
v https://coinmarketcap.com/currencies/bitcoindark/