Roadmaps

v1.5.4

Point #2-#6

#2. Replace OpenSSL with libsecp256k1

OpenSSL have caused chain splits, so bitcoin core dropped OpenSSL and used libsecp256k1 for all signing/verification.

#3. Replace Berkeley DB with SQLite

but BDB for the block index and wallet was removed in Bitcoin 0.8 (2013) because it caused chain split and BDB may be corrupted by unnormal shutdown.

#4. Signed variable overflows (int vs int64_t)

#5. Replace the threading/locking with a modern patterns

Threading/locking is the old, currently structure is not thread-safe, and depends on the lock orders.

#6. Multiple *.pro files in the project for each platform.

v1.5.5

Point #1 (modern bitcoin-core)

#1. replace bitcoin core from 14 years older version to the latest

v1.5.6

BIP-360 + #7-#11

BIP-360

Pre-requisites: SegWit, Bech32/m, Schnorr, Taproot, HD,

(BIP-141, 143, 144, 147, 173, 350, 340, 341, 342, 32, 44)

The point #1 (moderized bitcoin core) does include all pre-requisites for BIP-360.

#7-#11

#7. Scrypt.cpp is dangerous, it's allocating too many memory in the stack (not heap memory)

Potentially stack overflow

#8. scypt is depricated, because it can't use the modern CPU capabilities at all (AVX2/AVX-512/NEON v8...)

scrypt is used for hashing block headers and wallet KDF.

It's deprecated.

- scrypt-x86_64.S is SSE2 implementation. It uses 128-bit XMM registers (movdqa, pxor, paddd, etc.). It does not use YMM (AVX, AVX2, 256-bit) or ZMM (AVX-512, 512-bit) registers.

- scrypt-arm.S is the NEONv7 32-bit ARM implementation (q0–q15 128-bit registers). It does not use ARMv8 AArch64 NEON, SVE, or SVE2.

- scrypt-x86.S is the 32-bit SSE2 fallback.

#9. irc.cpp connects to irc.lfnet.org (and a hardcoded IP 92.243.23.21 as fallback), it can be injected. and the protocol is unencrypted IRC over port 6667.

#10. ntp.cpp runs ThreadNtpSamples which queries random NTP servers

NTP traffic is unauthenticated UDP. Anyone in path can spoof a response. NIST and Apple servers don't sign NTP packets in the default mode.

#11. Wallet KDF iteration count is 1000–10000× too low for now

// 25000 rounds is just under 0.1 seconds on a 1.86 GHz Pentium M

It's too old code part.

Point #12, Point #13 is for the DevOps, not release