```
BIP: 320
Title: nVersion bits for general purpose use
Author: BtcDrak <btcdrak@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0320
Status: Draft
Type: Standards Track
Created: 2018-03-01
License: BSD-3-Clause
         CC0-1.0
```

Abstract

This BIP reserves 16 bits of the block header nVersion field for general purpose use and removes their meaning for the purpose of version bits soft-fork signalling.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

Motivation

There are a variety of things that miners may desire to use some of the nVersion field bits for. However, due to their use to coordinate miner activated soft-forks, full node software will generate false warnings about unknown soft forks if those bits are used for non soft fork signalling purposes. By reserving bits from the nVersion field for general use, node software can be updated to ignore those bits and therefore will not emit false warnings. Reserving 16 bits for general use leaves enough for 13 parallel soft-forks using version bits.

Example Uses

The following are example cases that would benefit from using some of the bits from the nVersion field. This list is not exhaustive.

Bitcoin mining hardware currently can exhaust the 32 bit nonce field in less than 200ms requiring the controller to distribute new jobs very frequently to each mining chip consuming a lot of bandwidth and CPU time. This can be greatly reduced by rolling more bits. Rolling too many bits from nTime is not ideal because it may distort the timestamps over a longer period.

Version-rolling AsicBoost requires two bits from the nVersion field to calculate 4-way collisions. Any two bits can be used and mining equipment can negotiate which bits are to be used with mining pools via the Stratum "version-rolling" extension.

Specification

Sixteen bits from the block header nVersion field, starting from 13 and ending at 28 inclusive (0x1fffe000), are reserved for general use and removed from BIP8 and BIP9 specifications. A mask of 0xe0001fff should be applied to nVersion bits so bits 13-28 inclusive will be ignored for soft-fork signalling and unknown soft-fork warnings.

This specification does not reserve specific bits for specific purposes.

Reference Implementation

https://github.com/btcdrak/bitcoin/commit/d12516e136d4a8952904a13eedc9f4225f35dc3b

Backwards Compatibility

Non-upgraded nodes will interpret the reserved bits of this proposal as signals for soft forks, and may additionally activate the warning system for unknown soft forks.

This proposal does not require a soft fork to implement.

At the time of writing no known soft forks are pending using any of 16 bits reserved in this BIP, and given that a non-trivial percentage of the hashrate is already making uses of those bits, future soft forks SHOULD NOT utilise those bits for activation signalling.

Acknowledgements

Timo Hanke and Sergio Lerner for originally proposing 15-bit extra nNonce2.

References

BIP8

BIP9

AsicBoost white paper

Blockheader Extra nNonce2 proposal

Stratum protocol extension BIP for version-rolling

Copyright