```
BIP: 109
Layer: Consensus (hard fork)
Title: Two million byte size limit with sigop and sighash limits
Author: Gavin Andresen <gavinandresen@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0109
Status: Rejected
Type: Standards Track
Created: 2016-01-28
License: PD
```

Abstract

One-time increase in total amount of transaction data permitted in a block from 1MB to 2MB, with limits on signature operations and hashing.

Motivation

1. Continue current economic policy.
2. Exercise hard fork network upgrade.
3. Mitigate potential CPU exhaustion attacks

Specification

MAX_BLOCK_SIZE increased to 2,000,000 bytes

The maximum number of bytes in a canonically serialized block shall be increased from 1,000,000 bytes to 2,000,000 bytes.

Switch to accurately-counted sigop limit of 20,000 per block

The existing MAX_SIGOPS limit of 20,000 signature operations per block shall be retained, but only ECDSA verifications actually performed to validate the block shall be counted.

In particular:

- The coinbase scriptSig is not counted
- Signature operations in un-executed branches of a Script are not counted
- OP_CHECKMULTISIG evaluations are counted accurately; if the signature for a 1-of-20 OP_CHECKMULTISIG is satisified by the public key nearest the top of the execution stack, it is counted as one signature operation. If it is satisfied by the public key nearest the bottom of the execution stack, it is counted as twenty signature operations.
- Signature operations involving invalidly encoded signatures or public keys are not counted towards the limit

Add a new limit of 1,300,000,000 bytes hashed to compute transaction signatures per block

The amount of data hashed to compute signature hashes is limited to 1,300,000,000 bytes per block. The same rules for counting are used as for counting signature operations.

Activation: 75% hashpower support trigger, followed by 28-day 'grace period'

Solo miners or mining pool operators express their support for this BIP by setting the fourth-highest-bit in the block's 32-bit version number (0x10000000 in hex). The first block with that bit set, a timestamp less than or equal to the expiration time, and with at least 750 out of 1000 blocks preceding it (with heights H-1000..H-1) with that bit set, shall define the beginning of a grace period. Blocks with timestamps greater than or equal to the triggering block's timestamp plus 28 days (60*60*24*28 seconds) shall be subject to the new limits.

As always, miners are expected to use their best judgement for what is best for the entire Bitcoin ecosystem when making decisions about what consensus-level changes to support.

Expiration: 1-Jan-2018

If this BIP is not triggered before 1-Jan-2018 00:00:00 GMT it should be considered withdrawn.

Miners that support this BIP should set bit 0x10000000 in the block version until 1-Jan-2018. After that date, that bit can be safely re-used for future consensus rule upgrades.

Backward compatibility

Fully validating older clients are not compatible with this change. The first block exceeding the old limits on block size or inaccurately counted signature operations will partition older clients off the new network.

SPV (simple payment validation) wallets are compatible with this change.

Rationale

In the short term, an increase is needed to handle increasing transaction volume.

The limits on signature operations and amount of signature hashing done prevent possible CPU exhaustion attacks by "rogue miners" producing very expensive-to-validate two megabyte blocks. The signature hashing limit is chosen to be impossible to reach with any non-attack transaction or block, to minimize the impact on existing mining or wallet software.

The choices of constants for the deployment scheme were motivated by prior experience with upgrades to the Bitcoin consensus rules:

- 0x10000000 was chosen to be compatible with the BIP 9 proposal for parallel deployment of soft forks
- 75% was chosen instead of 95% to minimize the opportunity for a single large mining pool or miner to be able to veto an increase, either because of ideological opposition or threat of violence or extortion.
- A four-week grace period after the voting period was chosen as a balance between giving people sufficient time to upgrade and keeping people's attention on the urgent need to upgrade.

Implementation

https://github.com/gavinandresen/bitcoin-git/tree/two_mb_bump

See also http://gavinandresen.ninja/a-guided-tour-of-the-2mb-fork

Copyright