Abstract

Replace the static 1M block size hard limit with a hard limit set by coinbase vote, conducted on the same schedule as difficulty retargeting.

Motivation

Miners directly feel the effects, both positive and negative, of any maximum block size change imposed by their peers. Larger blocks allow more growth in the on-chain ecosystem, while smaller blocks reduce resource requirements network-wide. Miners also act as an efficient proxy for the rest of the ecosystem, since they are paid in the tokens collected for the blocks they create.

A simple deterministic system is specified, whereby a 75% mining supermajority may activate a change to the maximum block size each 2016 blocks. Each change is limited to a 5% increase from the previous block size hard limit, or a decrease of similar magnitude. Among adopting nodes, there will be no disagreement on the evolution of the maximum block size.

The system is compatible with emergent consensus, but whereas under that system a miner may choose to accept any size block, a miner following BIP100 observes the 75% supermajority rule, and the 5% change limit rule. Excessive-block values signaled by emergent consensus blocks are considered in the calculation of the BIP100 block size hard limit, and the BIP100 calculated maximum block size is signaled as an excessive-block value for the benefit of all observers.

Specification

Dynamic Maximum Block Size

1. Initial value of `hardLimit` is 1000000 bytes, preserving current system.
2. Changing `hardLimit` is accomplished by encoding a proposed value, a vote, within a block's coinbase scriptSig, and by processing the votes contained in the previous retargeting period.

\# Vote encoding

(a) i. A vote is represented as a megabyte value using the BIP100 pattern

    `/BIP100/B[0-9]+/`

    Example: `/BIP100/B8/` is a vote for a 8000000-byte `hardLimit`.

  ii. If the block height is encoded at the start of the coinbase scriptSig, as per BIP34, it is ignored.

  iii. Only the first BIP100 pattern match is processed in "Maximum block size recalculation" below.

  iv. A megabyte value is represented by consecutive base-ten digits.

  v. If no BIP100 pattern is matched, the first matching emergent consensus pattern `/EB[0-9]+/`, if any, is accepted as the megabyte vote.

(b) Maximum block size recalculation

  i. A `new hardLimit` is calculated after each difficulty adjustment period of 2016 blocks, and applies to the next 2016 blocks.

  ii. Absent/zero-valued votes are counted as votes for the `current hardLimit`.

  iii. The votes of the previous 2016 blocks are sorted by megabyte vote.

  iv. Raising `hardLimit`

    \# The `raise value` is defined as the vote of the 1512th highest block, converted to bytes.

    A. If the resultant `raise value` is greater than (`current hardLimit` * 1.05) rounded down, it is set to that value.

    B. If the resultant `raise value` is greater than `current hardLimit`, the `raise value` becomes the `new hardLimit` and the recalculation is complete.

  v. Lowering `hardLimit`

    \# The `lower value` is defined as the vote of the 1512th lowest block, converted to bytes.

    A. If the resultant `lower value` is less than (`current hardLimit` / 1.05) rounded down, it is set to that value.

    B. If the resultant `lower value` is less than `current hardLimit`, the `lower value` becomes the `new hardLimit`

and the recalculation is complete.

vi. Otherwise, `new hardLimit` remains the same as `current hardLimit`.

Signature Hashing Operations Limits

1. The per-block signature hashing operations limit is scaled to (actual block size, fractional megabyte rounded to next higher megabyte) / 50.
2. A maximum serialized transaction size of 1000000 bytes is imposed.

Recommendations

Publication of `hardLimit`

1. For the benefit of all observers, it is recommended that `hardLimit` be published. Example: a complete coinbase string might read

   `/BIP100/B8/EB2.123456/`

   which indicates a vote for 8M maximum block size, and an enforced `hardLimit` of 2.123456 megabytes for the block containing the coinbase string.

Deployment

This BIP is presumed deployed and activated as of block height 449568 by implementing nodes on the bitcoin mainnet. It has no effect until a raise value different from 1M is observed, which requires at least 1512 of 2016 blocks to vote differently from 1M.

Backward compatibility

The first block larger than 1M will create a network partition, as nodes with a fixed 1M hard limit reject that block.

Implementations

https://github.com/bitcoinxt/bitcoinxt/pull/188 https://github.com/bitcoinxt/bitcoin/pull/1 https://github.com/BitcoinUnlimited/BitcoinUnlimited/pull/398

Copyright