

BIP: 105
Layer: Consensus (hard fork)
Title: Consensus based block size retargeting algorithm
Author: BtcDrak <btcdrak@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: <https://github.com/bitcoin/bips/wiki/Comments:BIP-0105>
Status: Rejected
Type: Standards Track
Created: 2015-08-21
License: PD

Abstract

A method of altering the maximum allowed block size of the Bitcoin protocol using a consensus based approach.

Motivation

There is a belief that Bitcoin cannot easily respond to raising the blocksize limit if popularity was to suddenly increase due to a mass adoption curve, because co-ordinating a hard fork takes considerable time, and being unable to respond in a timely manner would irreparably harm the credibility of bitcoin.

Additionally, predetermined block size increases are problematic because they attempt to predict the future, and if too large could have unintended consequences like damaging the possibility for a fee market to develop as block subsidy decreases substantially over the next 9 years; introducing or exacerbating mining attack vectors; or somehow affect the network in unknown or unpredicted ways. Since fixed changes are hard to deploy, the damage could be extensive.

Dynamic block size adjustments also suffer from the potential to be gamed by the larger hash power.

Free voting as suggested by BIP100 allows miners to sell their votes out of band at no risk, and enable the sponsor the ability to manipulate the blocksize. It also provides a cost free method for the larger pools to vote in ways to manipulate the blocksize such to disadvantage or attack smaller pools.

Rationale

By introducing a cost to increase the block size ensures the mining community will collude to increase it only when there is a clear necessity, and reduce it when it is unnecessary. Larger miners cannot force their wishes so easily because not only will they have to pay extra a difficulty target, then can be downvoted at no cost by the objecting hash power.

Using difficulty as a penalty is better than a fixed cost in bitcoins because it is less predictable.

In order to prevent miners having complete control over blocksize, an upper limit is required at protocol level. This feature ensures full nodes retain control over consensus, remembering full nodes are the mechanism to keep miners honest.

Specification

The initial block size limit shall be 1MB.

Each time a miner creates a block, they may vote to increase or decrease the blocksize by a maximum of 10% of the current block size limit. These votes will be used to recalculate the new block size limit every 2016 blocks.

Votes are cast using the block's coinbase transaction scriptSig.

As per BIP34, the coinbase transaction scriptSig starts with a push of the block height. The next push is a little-endian number representing the preferred block size in bytes. For example, 0x4c(OP_PUSHDAT1) 0x03(size of constant) 0x80 0x84 0x1e(2MB) or 0x4c(OP_PUSHDAT1) 0x04(size of constant) 0x80 0x96 0x98 0x00(10MB).

If a miner votes for an increase, the block hash must meet a difficulty target which is proportionally larger than the standard difficulty target based on the percentage increase they voted for.

Votes proposing decreasing the block size limit do not need to meet a higher difficulty target.

Miners can vote for no change by voting for the current block size.

For blocks to be valid the blockhash must meet the required difficulty target for the vote otherwise the block is invalid and will be rejected.

Every 2016 blocks, the block size limit will be recalculated by the median of all votes in the last 2016 blocks. This will redefine the block size limit for the next 2016 blocks.

Blocks that are larger than the calculated base block size limit are invalid and will be rejected.

The base block size limit may not reduce below 1MB or increase above 8MB (the exact number for the upper limit requires further discussion).

Acknowledgements

This proposal is based on ideas and concepts derived from the writings of Meni Rosenfeld and Gregory Maxwell.

References

BIP34

Copyright

This work is placed in the public domain.