```
BIP: 103
Layer: Consensus (hard fork)
Title: Block size following technological growth
Author: Pieter Wuille <pieter.wuille@gmail.com>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0103
Status: Withdrawn
Type: Standards Track
Created: 2015-07-21
License: BSD-2-Clause
```

Abstract

This BIP proposes a block size growth intended to accommodate for hardware and other technological improvements for the foreseeable future.

Copyright

Motivation

Many people want to see Bitcoin scale over time, allowing an increasing number of transactions on the block chain. It would come at an increased cost for the ecosystem (bandwidth, processing, and storage for relay nodes, as well as an impact on propagation speed of blocks on the network), but technology also improves over time. When all technologies depended on have improved as well as their availability on the market, there is no reason why Bitcoin's fundamental transaction rate cannot improve proportionally.

Currently, there is a consensus rule in place that limits the size of blocks to 1000000 bytes. Changing this requires a hard-forking change: one that will require every full node in the network to implement the new rules. The new chain created by those changed nodes will be rejected by old nodes, so this would effectively be a request to the ecosystem to migrate to a new and incompatible network. Doing this while controversy exists is dangerous to the network and the ecosystem.

Furthermore, the effective space available is always constrained by a hash rate majority and its ability to process transactions. No hard forking change that relaxes the block size limit can be guaranteed to provide enough space for every possible demand - or even any particular demand - unless strong centralization of the mining ecosystem is expected. Because of that, the development of a fee market and the evolution towards an ecosystem that is able to cope with block space competition should be considered healthy. This does not mean the block size or its limitation needs to be constant forever. However, the purpose of such

a change should be evolution with technological growth, and not kicking the can down the road because of a fear of change in economics.

Bitcoin's advantage over other systems does not lie in scalability. Well-designed centralized systems can trivially compete with Bitcoin's on-chain transactions in terms of cost, speed, reliability, convenience, and scale. Its power lies in transparency, lack of need for trust in network peers, miners, and those who influence or control the system. Wanting to increase the scale of the system is in conflict with all of those. Attempting to buy time with a fast increase is not wanting to face that reality, and treating the system as something whose scale trumps all other concerns. A long term scalability plan should aim on decreasing the need for trust required in off-chain systems, rather than increasing the need for trust in Bitcoin.

In summary, hard forks are extremely powerful, and we need to use them very responsibly as a community. They have the ability to fundamentally change the technology or economics of the system, and can be used to disadvantage those who expected certain rules to be immutable. They should be restricted to uncontroversial changes, or risk eroding the expectation of low trust needed in the system in the longer term. As the block size debate has been controversial so far - for good or bad reasons - this BIP aims for gradual change and its effects start far enough in the future.

Specification

The block size limitation is replaced by the function below, applied to the median of the timestamps of the previous 11 blocks, or in code terms: the block size limit for pindexBlock is GetMaxBlockSize(pindexBlock->pprev->GetMedianTimePast()).

The sigop limit scales proportionally.

It implements a series of block size steps, one every ~97 days, between January 2017 and July 2063, each increasing the maximum block size by 4.4%. This allows an overall growth of 17.7% per year.

```
uint32_t GetMaxBlockSize(int64_t nMedianTimePast) {
    // The first step is on January 1st 2017.
    if (nMedianTimePast < 1483246800) {
        return 1000000;
    }
    // After that, one step happens every 2^23 seconds.
    int64_t step = (nMedianTimePast - 1483246800) >> 23;
    // Don't do more than 11 doublings for now.
    step = std::min<int64_t>(step, 175);
    // Every step is a 2^(1/16) factor.
    static const uint32_t bases[16] = {
        // bases[i] == round(1000000 * pow(2.0, (i + 1) / 16.0))
```

```
        1044274, 1090508, 1138789, 1189207,
        1241858, 1296840, 1354256, 1414214,
        1476826, 1542211, 1610490, 1681793,
        1756252, 1834008, 1915207, 2000000
    };
    return bases[step & 15] << (step / 16);
}
```

Rationale

Waiting 1.5 years before the hard fork takes place should provide ample time to minimize the risk of a hard fork, if found uncontroversial.

Because every increase (including the first) is only 4.4%, risk from large market or technological changes is minimized.

The growth rate of 17.7% growth per year is consistent with the average growth rate of bandwidth the last years, which seems to be the bottleneck. If over time, this growth factor is beyond what the actual technology offers, the intention should be to soft fork a tighter limit.

Using a time-based check is very simple to implement, needs little context, is efficient, and is trivially reviewable. Using the "median time past" guarantees monotonic behaviour, as this median is required to be increasing, according to Bitcoin's existing consensus rules. Using the "median time past" of the block before means we know in advance what the limit of each block will be, without depending on the actual block's timestamp.

Compatibility

This is a hard forking change, thus breaks compatibility with old fully-validating node. It should not be deployed without widespread consensus.

Acknowledgements

Thanks to Gregory Maxwell and Wladimir J. van der Laan for their suggestions.