A flexible limit: trading subsidy for larger blocks

Mark Friedenbach
Scaling Bitcoin Hong Kong
7 Dec 2015

The Need for Dynamic Block Size

- Too small of a block size limit results in inaccessible payment network (useless).
- Too large of a block size limit results in centralization pressures (loss of value).
- The “Goldilocks” (金发姑娘和三只熊) limit is the largest block size that still allows a decentralized network.

The Need for Dynamic Block Size

- BIP 101, 103, … :
  Block size automatically increases according to a fixed schedule. If too large too fast, large miners can force small ones into unprofitability.
- BIP 100, 105, … :
  Block size determined by miner vote, but what makes miners' interests align with other users' interests? A small (33%) cabal can steal the vote.
- Solution: economic costs to voting ensure profit-seeking miners reflect user demand.

The Need for Dynamic Block Size

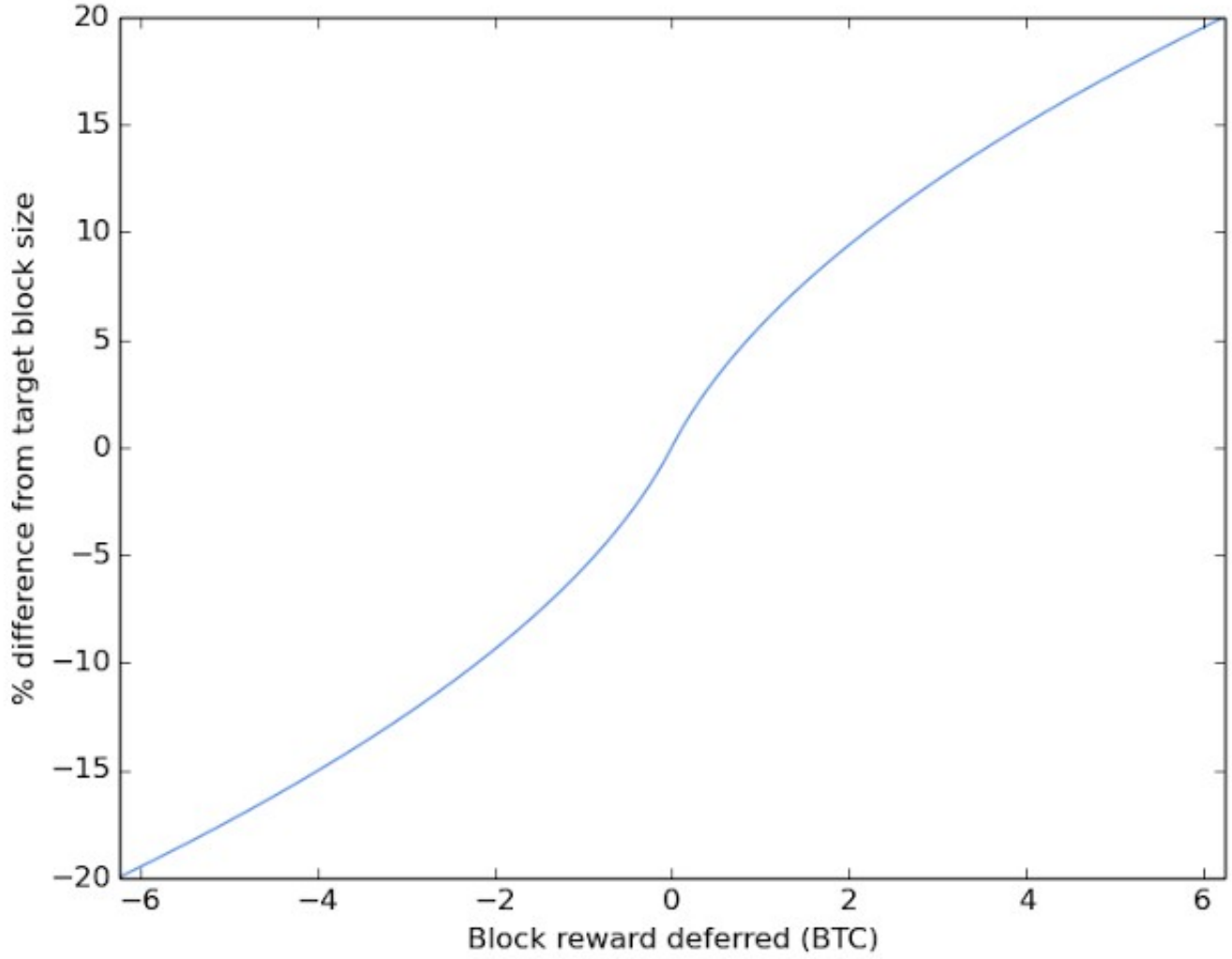
- We cannot predict with accuracy what parameters will be safe far in advance.
- Capacity limits need to expand to meet actual demand, by a method that is adversarially secure.
- Measurements of demand must involve scarce resources (e.g. hashpower, block reward, bitcoin days destroyed) to ensure a cost to attackers.

A Flexible Block Size Limit

- To increase: defer part of the block reward.
- To decrease: reclaim previously deferred reward.
- Periodically adjust base limit based on how much block reward was deferred over last 2016 blocks.
- Allow users to increase or decrease sensitivity via bitcoin-days-destroyed weighted votes.

- Flexcap: Meni Rosenfeld and Gregory Maxwell
  Voting scheme: Jeff Garzik and Peter Todd

A Flexible Block Size Limit: Graphs



A Flexible Block Size Limit: Code

- factor = sqrt(40,955x + 67,092,481) – 8,191
  In: 0..24573 Out: 0..24573
- The Dijkstra integer sqrt implementation is quantized over 30-bit integers.
- Constant factors and shifts are selected to provide a function with a first derivative of 0.5 at the start of the input range, and 0.125 (a decrease of 4x) at the end.
- https://github.com/maaku/bitcoin/tree/flexcap

Adjustable Security Parameter

- The maximum allowed deferred subsidy sets the marginal cost of a percent of added block space.
- Optimal setting depends on present subsidy, price of bitcoin, and subjective determination of health of network.
- Seemingly impossible to automatically determine from data available to the consensus layer.

Adjustable Security Parameter: User Votes

- Periodically adjust security parameter (cost per %increase) up or down based vote signaled in txns.
- Use bitcoin-days-destroyed as weighting factor: of the scarce resources available, bitcoin-days is the most aligned with stakeholder importance.
- txin.nSequence:

  0b111111111 11111111 11111111 11111111

  0b010000000 00000000 00000000 00000000 ✓

  0b001000000 00000000 00000000 00000000 ✗

  0b000000000 00000000 00000000 00000000

Future Work & Request for Collaborations

- Determine adjustment formula and weighting function for security parameter user voting.
- Perform simulations, and back-testing using Rusty's block+mempool corpus.
- Draft BIP & deployment code.
- Find me during the sprints!

Mark Friedenbach
CD879A60 489CD6FA FD8D6F4F 88BD99BF 46BB9B3D