

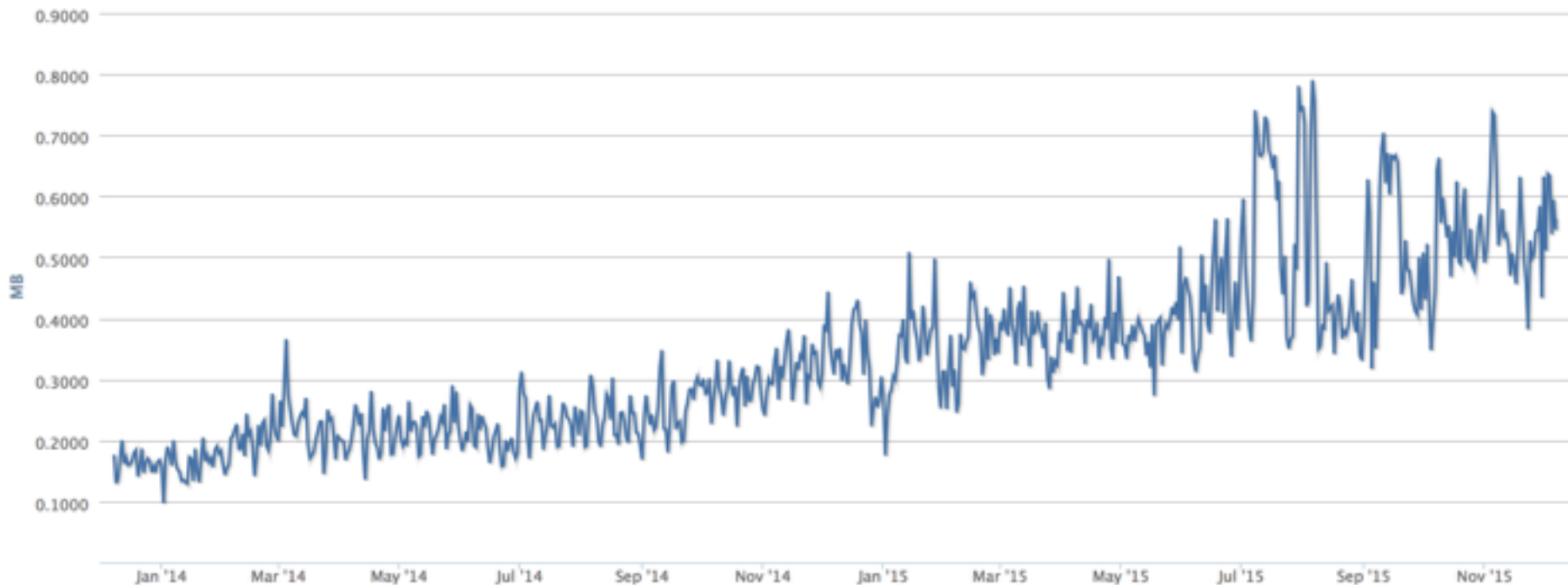
An aerial night view of a city grid, likely New York City, with the word "blog" overlaid in a blue, lowercase, sans-serif font. The city lights are visible, and the sky is a mix of blue and purple hues.

blog

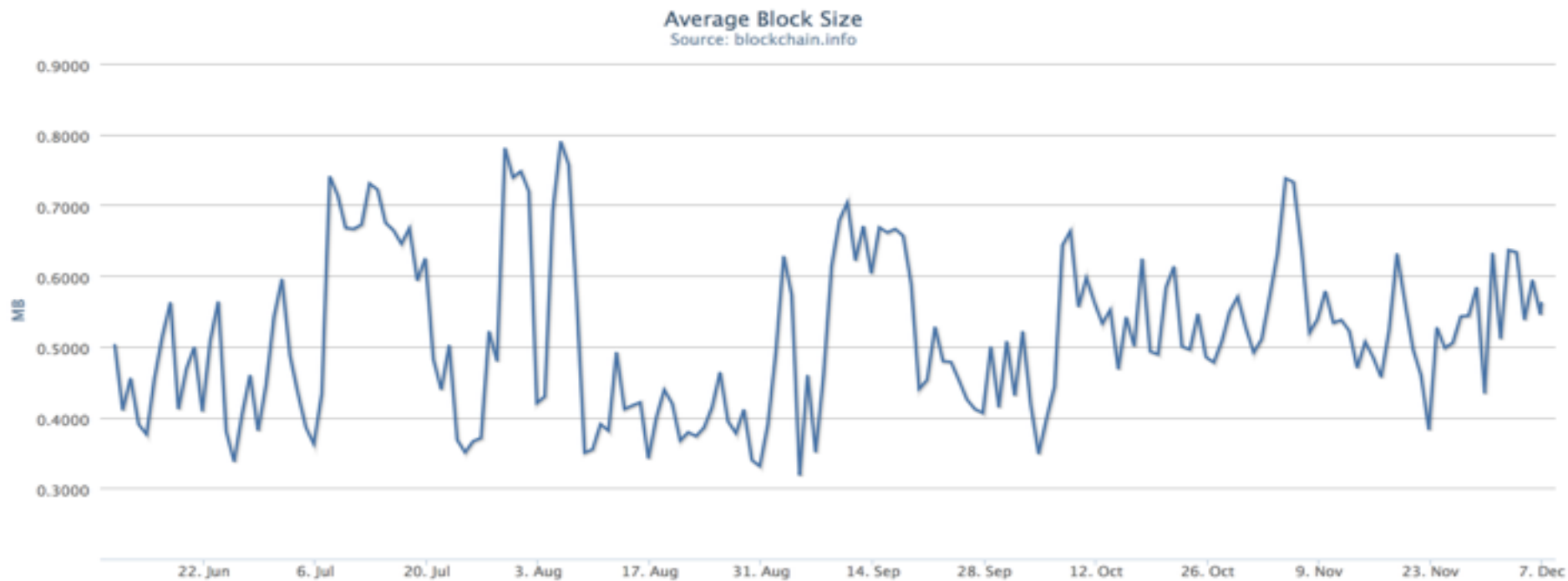
A Bevy of Block Size Proposals
Dec. 2015

- Actively addressing technical scaling issues — good
- Deferring economics and game theory issues — not good
- FOMC Problem: Humans pick block size (= choose economics)
 - vs Free Market problems: block size poorly chosen
- Centralization on low end and high end
 - Defeats security and privacy of system
- Where is a healthy fee market?
- Is the algorithm easy to manipulate (game)?
- Little field data on hard forks — just theories & predictions
- Signaling bitcoin growth to external parties, current bitcoin users
- Predictability of block size and fee market, from user PoV
- Miners mining without validating (SPV mining)
- Miners can soft-fork into block size reduction

Average Block Size - Past 2 years



Average Block Size - Past 180 days



- User Experience
 - Fees are very difficult to reason and predict, by design
 - Fees disconnected from transaction value - size-based
 - High fee might result in long wait; no guarantee of next block
 - 4 choices: ASAP, average, below average, long wait
- Fee market status, changes, economics, market reaction
 - Fee market exists in narrow band based on dumb wallet software fee behavior + miner latency
 - Scenario: Full blocks + block size change
 - Scenario: Not-full blocks + block size change
 - Large block size step reboots fee market

- **Theme: “Shift block size from devs to free market”**
- Limit floats between 1M and 32M
 - Training wheels - more hard forks required to move beyond
- Default growth: 1.09% per diff period (100% every 2.5 years)
- “Slow motion miner vote”
 - Continuous 3-window voting window
 - At each 2wk diff period, new size from last 3 months’ coinbases
 - Blocksize: Examine 90th percentile of votes, take average
- Limit may not increase or decrease more than 1.2x in one period
- Activation: Flag day X, after which miner voting is examined

- Analysis
 - Shifts block size selection to free market
 - Avoids anointing devs as new FOMC
 - Miners have input on fee income
- Community Feedback
 - Gives miners have too much control
 - Miners can sell votes costlessly
 - Limit increase too large (addressed)

- **Theme: “Predictable growth”**
- Immediate jump to 8M
- Double every 2 years
- Activation: 750 of 1,000 blocks indicate support, + 2 week grace

- Analysis
 - Predictable
 - No free market sensitivity
 - Fee market significantly postponed
- Feedback
 - Big size bump
 - Appears larger than current consensus
 - Community reaction to Bitcoin-XT (not BIP 101)
 - Community reaction: Open letters tossed back & forth

- **Theme: Block size following technological growth**
- Increase size by 4.4% every 97 days (17.7% growth/year)
- Activation: Jan 1, 2017 (1.5 years away)

- Analysis
 - Predictable
 - No free market sensitivity
 - Fee market sooner
- Feedback
 - Sparse community feedback
 - Way too small an increase
 - Another hard fork likely required to adapt system
 - Activation in 2017 too far away

- **Theme: Consensus based block size retargeting**
- Start at 1M
- Miners vote to +/- block size by maximum of 10% per diff period
- Miners vote by providing proportionally larger block hash target
- Activation: Not specified

- Analysis
 - Shifts block size selection to free market
 - Avoids anointing devs as new FOMC
 - Miners have input on fee income
- Community Feedback
 - Very little feedback
 - Pay-with-difficulty skews incentives, difficult for miners to reason

Honorable mention: Pay-to-future-miner (Meni R.)

- **Theme: Dynamically controlled block size max cap**
- Variant #1:
 - Per diff period; *first* 2000 blocks of diff period examined.
 - If 90% of blocks higher than 90% full, block size 2x
 - If 90% of blocks less than 50% full, block size 1/2
 - Otherwise, no change
- Variant #2:
 - Examine last 2 diff periods
 - Formula too complex to fit on slide :)
 - If TX fee pressure increases, increase block size
- Activation: not specified

- Analysis
 - Shifts block size selection to free market
 - Avoids anointing devs as new FOMC
- Community Feedback
 - Sparse community feedback
 - Variant #1
 - Huge steps
 - Easily gamed
 - Variant #2:
 - More interesting
 - Encoded economics of “too much fee pressure”

- **Theme: “The Backup Plan”**
- One-time bump to 2M
- Activation: Flag day X, with non-binding miner voting

- Analysis
 - Intended as backup option, vs. other BIPs
 - Conservative, vis block size limit
 - Conservative, vis block size algorithm
 - Conservative method of obtaining hard fork field data
 - Highly predictable (“always 2M”)
 - No free market sensitivity
- Feedback
 - 2M seems generally acceptable
 - Does not avoid “FOMC problem” (humans picking numbers)
 - Requires another hard fork to move beyond

- **Theme: “2-4-8”**
- 2M now
- 4M in 2 yrs
- 8M in 4yrs
- Activation: Flag day X + non-binding miner voting (presumed)

*Not an official BIP number; as proposed by Adam Back

- Analysis
 - Conservative, vis block size limit
 - Conservative, vis block size algorithm
 - Conservative method of obtaining hard fork field data
 - Highly predictable
 - No free market sensitivity
- Feedback
 - Seems generally acceptable
 - Does not avoid “FOMC problem” (humans picking numbers)
 - Requires another hard fork to move beyond

- **Theme: Keep current block size - 1M - until change is “obviously necessary”**
- Keep current block size limit
- Keep node count decline rate at current levels

- Analysis
 - Maximally conservative - for the moment; no hard fork.
 - Current working system keeps working (until blocks are full)
- Feedback
 - Goes against economic majority of bitcoin businesses & miners
 - Once blocks are full,
 - Radical change to more-adversarial, zero-sum system
 - Radical change to fee market - users priced out of system
 - Wallet software poorly prepared - poor UX
 - No apparent growth plan to outsiders -> avoid bitcoin altogether
 - Crisis based change gives users more unpredictable system
 - No data gathered on hard fork until crisis
 - Centralization at low end

Personal thoughts and recommendations:

- Speaking only for myself — vendor hats off.
- **“Small bump now”** — Gather crucial field data, for future changes
 - “The Internet is the best test lab in the world”
- Plan now, code now, activate in T+6 months
- Economic consensus wants to push beyond 1M
- Technical consensus: Beyond 2M is risky today
- BIP 000 **do-nothing approach worst of all options**
 - Very poor future signaling to users, future users, market
 - Seems likely to fracture bitcoin
- Unresolved: How much fee is too much?
- Unresolved: Who decides how much fee is too much?

bloq

Thank You!

Jeff@Bloq.com

