Scaling Bitcoin workshop, Sept. 2015

Issues impacting Block Size proposals

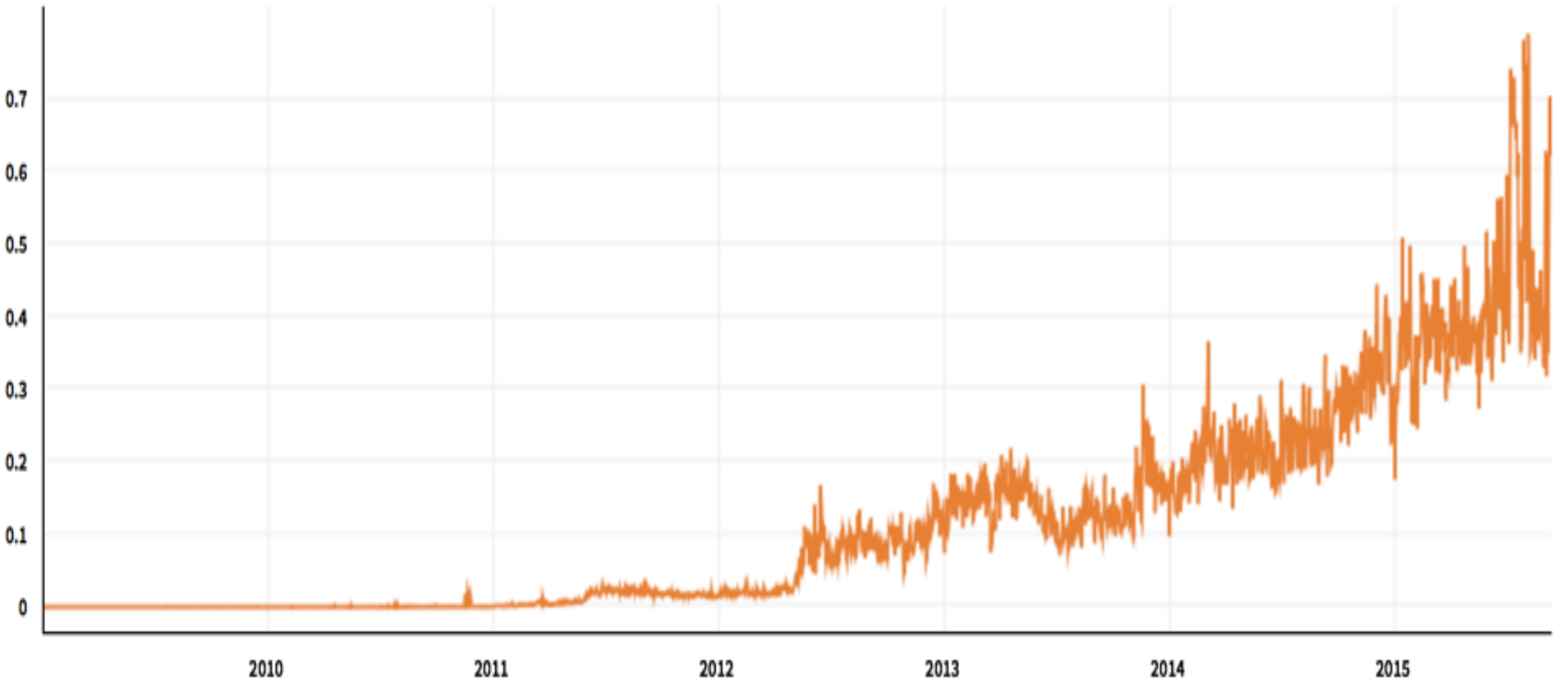
Jeff Garzik
Dunvegan Space Systems / BitPay

History

- Bitcoin introduced as P2P electronic cash payments
- 1M block size hard limit set for anti-spam purposes
  - Otherwise, trivial to create 32M+ blocks at low cost

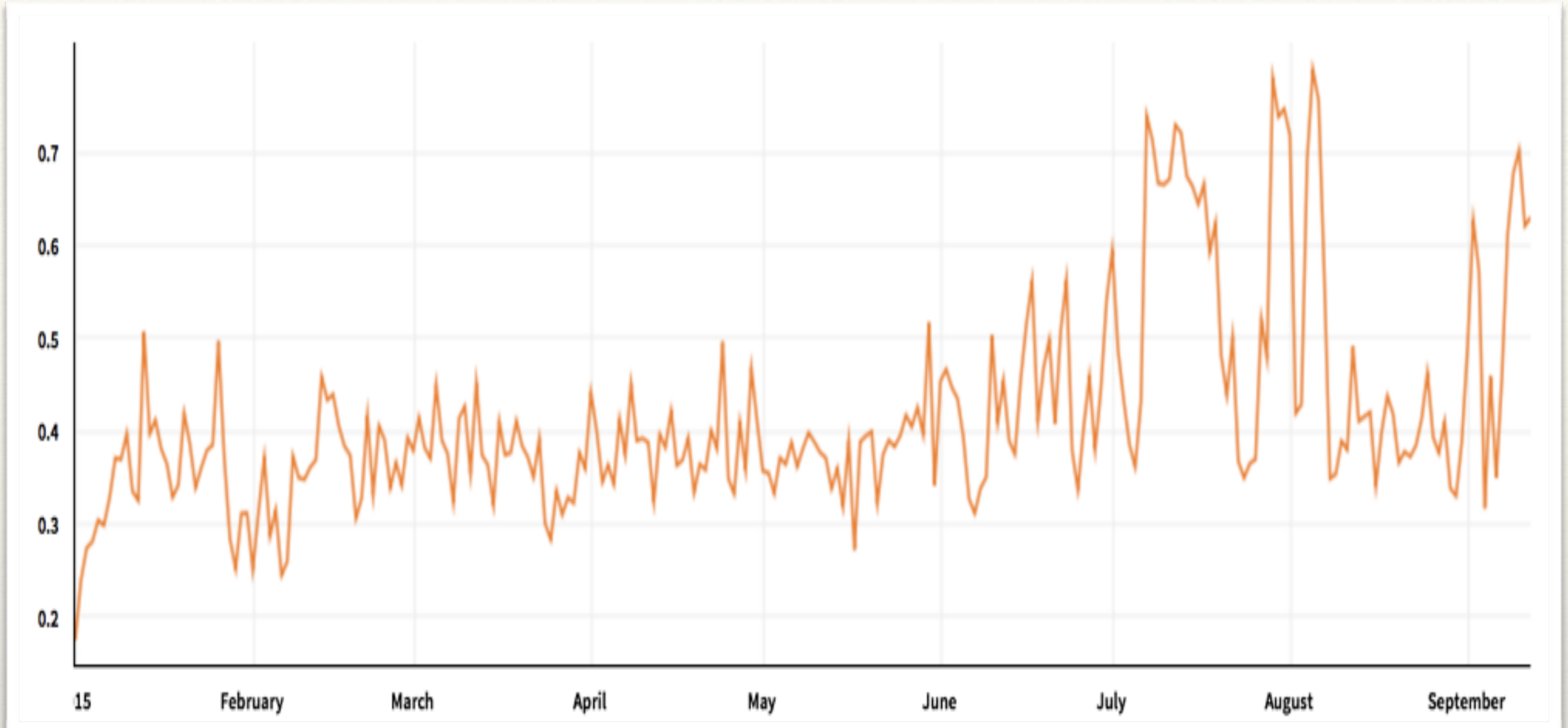
Observations - System

- Process of finding distributed consensus takes time
  - Bitcoin is a *settlement system*
    - Settles on a stable timeline of transactions
- Core service: **Censorship Resistance**
  - Enables permission-less innovation



Average Block Size

For all time



Average Block Size

Year 2015

Observations - Block Size

- Provides DoS protection. Raises Cost-Of-Attack.
- 250k soft limit: 0.1.0(?)
- 350k soft limit: 0.8.6 (Dec 2013)
- 750k soft limit: 0.9.0 (March 2014)
- Trend: Headed towards 1M hard limit
- Blocks not full today*
  - *Excluding long blocks, stress tests

Observations - Fee Market

- Zero fee competition*
  - *On average. Excludes long blocks, traffic bursts (stress tests), short periods prior to soft limit increase.
- Fee floor set by anti-“dust” relay limit
- Fees provide near-zero economic signaling today
  - Users: Fee choice depends on TX size and block size
    - Difficult to reason
  - Miners: Fees unpredictable; below noise level vs. 25 BTC subsidy

Observations 3

- Non-contentious hard fork: User voting mechanism
  - Check-and-balance
- Natural equilibrium block size exists, in absence of limit
- Rapid miner, mining pool turnover YoY
  - Permission-less miner entry

Problems 1: Wall at 1M

- **Major economic policy shift**, to fee competition
- Users, markets, software not prepared
  - UX rapidly degrades; erratic confirm times, fees.
    - Stress tests did force wallet authors to improve
- Market chaos as fees shift to new, higher equilibrium
- Event driven, not time driven (might precede HK)
- Businesses, users incentivized away by high fees

Problems 2 - High Level

- Stuck at 1M strangles bitcoin growth and adoption
- “Fidelity Problem”
  - Capacity projections impossible
  - Business plans never implemented
  - No user & traffic growth b/c few will build on BTC
    - Block size problem solves itself

Problems 3 - High Level

- Bitcoin built to be upgraded - must not get stuck at v1
- No good way to measure community opinion on blksz
- Getting stuck at 1M, due to hard fork contention
- Not thinking of the user & market experience
  - Fee market abruptly appears at 1M
    - Users not informed/prepared for new econ. policy
  - “Restore minimum feerate to 10000 satoshis” #6201

Problems 4 - Fee Market

- Market disruption upon shift to blocks-full-on-avg
  - Even worse: Not full(1M) - full (1M) - not full (2M)
- Zero fee competition
  - Moral hazard: Unsustainable long term(?)
    - Users hooked on low fees
  - Valid economic choice: subsidize adoption today

Problems 5 - Limit Increase Has Costs

- Hard fork required*
- Larger blocks push miners, nodes off system
- System security may be impacted
- Increased network load shouldered by ever-fewer actors

Problems 6

- Avoid high priests choosing magic values like 1M
- Avoid user cliffs (abrupt, large changes to market)
- “inv” storm response - Need BitTorrent-like throttling
- Centralization at low end (1M) and high end (1G)
- **Lack of data, field experience** on block size changes
  - Community likes safety rails
  - Simulations only go so far

Simulation variables

- L - Lightweight node count
- P - Pruned node count
- F - Full node count
- C - CPU cost for P, F to validate blocks
- D - Data storage costs
- N - Network resource cost for P/F relaying + L usage

Problems 7 - analysis errors

- Discounting or not seeing externalities
- Miners always maximize for fees
  - “If no size limit, miners never refuse a transaction”
- Miners must be profitable in the short term
- Possibility of selfish mining implies broken system

Observations

- Static, one-time increase: Need more forks later
- Static increase schedule: Might be too big or too small
- Feedback based: Reflects market; Possibly game-able
- Pay to future miner: Interesting
- Pay with difficulty: Scrambles incentives

Observations

- Prediction: 2nd “course correction” hard fork likely
- Do not plan, engineer too far into the future
- All The World’s Coffees will not fit on blockchain
- Limit increase needed to standard payment growth
- Limit increase also needed for payment channels, Lightning, side chains, other scaling methods.

Fini

Liberté, égalité, fraternité

JGarzik@DSS.co
JGarzik@BitPay.com