Alternatives to block size as aggregate resource limit

Mark Friedenbach
<mark@friedenbach.org>

Scaling Bitcoin Montréal, QC 2015

GPG: 5350 FF04 7067 0DEF A170
9D66 94F4 5E6A 5044 CE50

Background: why have a block size?

- **Place a finite upper bound on resources required to validate a Bitcoin block**

1) A hard upper bound on size of buffers during block transmission and validation (engineering considerations, primarily)

2) Rate-limit resource consumption during validation (achieve decentralization requirements)

3) Other limits e.g. MAX_BLOCK_SIGOPS derived from block size

Some problems emerge...

- **Block size correlates with resource consumption in the typical case**
  - But design criteria must be met even for worst-case, adversarial situations.
- **Specially constructed blocks can be made that require significantly more resources to validate than a typical 1MB block**
  - Observed in practice!
- **Actual limit must be constrained by worst-case scenario**
  - How much worse is the worst case?
  - Pretty bad, actually...

F2Pool spam cleanup

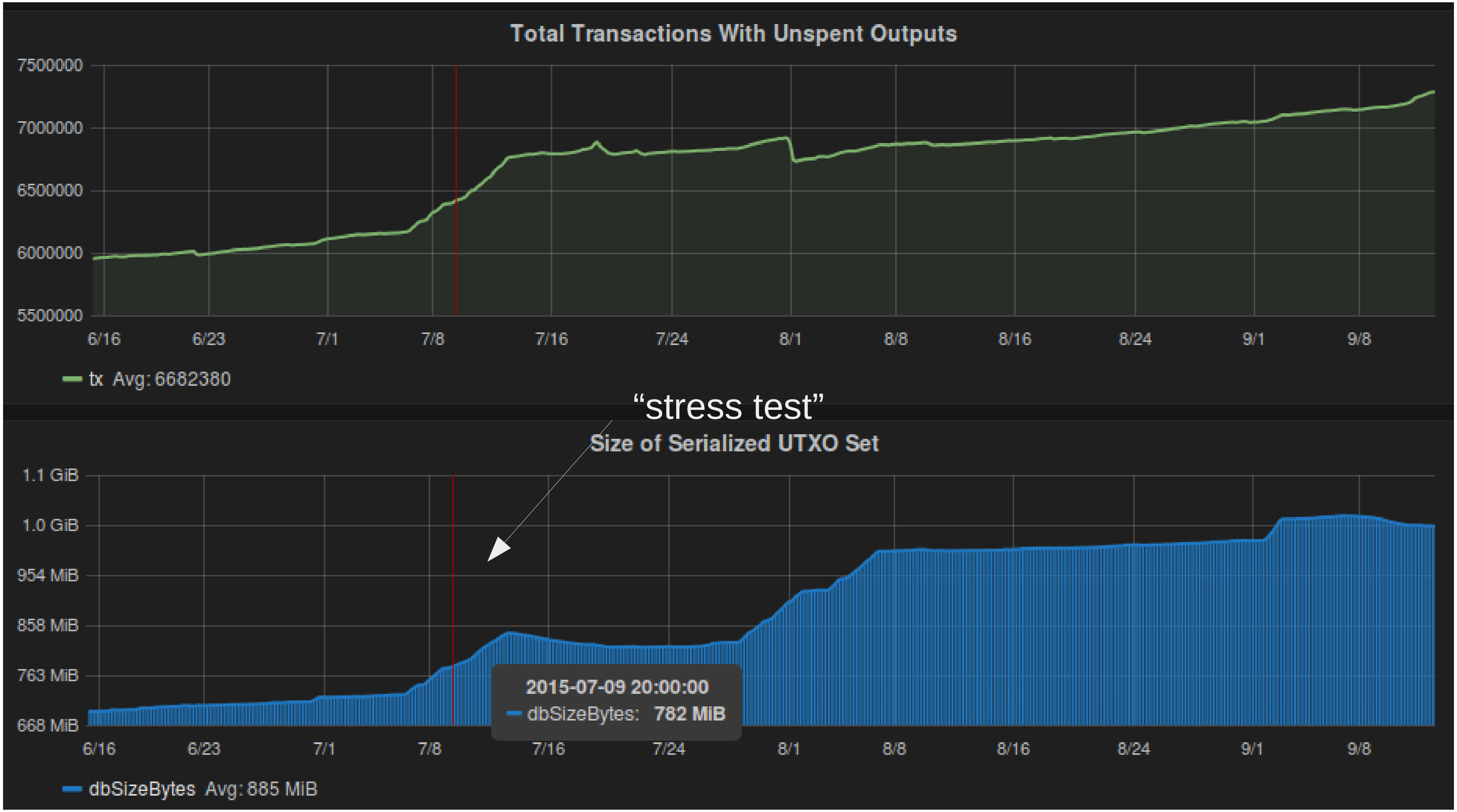
txid:bb41a757f405890fb0f5856228e23b715702d714d59bf2b1feb70d8b2b4e3e08

- **Block with only 1 non-coinbase transaction**
  - Sweeps 5569 dust UTXOs. Size: 999,657 bytes.
- **Transaction re-serialized for each signature check**
  - Total **1.25GB** of data serialized & hashed.
- **~30s to verify on actual nodes at the time.**
- **Scales as $O(n^2)$**
  - 3.2 MB: 10 min
  - 8.0 MB: 2 hr 8 min

MAX_BLOCK_SIGOPS *FAIL*
CVE 2013-2292

- **MAX_BLOCK_SIGOPS limits the aggregate number of signature checks in the outputs of a block...**
  - ...but it is the inputs, not outputs that are run.
- **Vulnerable to attack**
  - Over time create outputs with 200 CHECKSIG's each.
  - Spend all in one giant transaction.
  - MAX_BLOCK_SIGOPS does not apply.
- **“A transaction that takes at least 3 minutes to verify” (Sergio Damian Lerner, 30 Jan 2013) https://bitcointalk.org/?topic=140078**

UTXO set growth



“stress test”

http://statoshi.info/dashboard/db/unspent-transaction-output-set

How bad is it?

- **Worst case is pretty bad**
  - Between 10x – 100x slowdown from typical
  - Attacks are cheap (fees not linked to real costs)
  - $O(n^2)$ scaling gets worse with larger block size
  - Attacks observed in the wild!

We need a new measure of resource consumption that tracks validator costs more accurately than block size alone

Factors which affect full validation

- **Block size**
  - worst-case latency
- **UTXO growth**
  - created minus spent
- **Script...**
  - opcodes executed
  - space required
  - bytes copied
- **Elliptic curve operations**
  - In inputs, not outputs!
- **Bytes hashed**
  - Adjusted by algorithm?
- **Bytes copied**
  - OP_DUP...

A linear function of many variables

- **Infinite possible functions to consider**
  - Future work?
  - But...

- **A linear combination of factors**
  - Simplest commitment structure for fraud proofs (Merkle sum tree)
  - Straightforward, easy to implement solvers
  - Drop-in replacement in existing infrastructure

Selection of coefficients

- **Some factors are directly comparable**
  - Convert opcode execution counts, signature validations, and bytes hashed to single-threaded CPU running time.
- **Type error in some comparisons**
  - How many bytes of RAM equals 100 ms CPU utilization?
  - Use available server hardware to establish conversion ratios.
- **Factors grow differently over time**
  - Some factors expected to increase with Moore's law (parallel CPU speed).
  - Others expected to level out in the near future (global latency)

Summary & future work

- **Block size meant to rate-limit validater resource consumption**
  - Large resource usage causes propagation delays; delays cause centralization pressures.
- **Atypical blocks observed in the wild have widely varying resource usage**
  - Block size does poor job of predicting resource utilization & propagation delay in an adversarial environment.
- **Linear function of multiple factors ideal replacement for block size metric**
  - Simple, drop-in replacement for block size metric
  - Requires future work on finalizing set of factors and coefficients

Thank you!

Mark Friedenbach
<mark@friedenbach.org>

Scaling Bitcoin Montréal, QC 2015

GPG: 5350 FF04 7067 0DEF A170
9D66 94F4 5E6A 5044 CE50

See you in Hong Kong, Dec 2015!