Scaling Bitcoin

Ryan X. Charles
Blockchain University
Tokyo, Dec. 19, 2015

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Outline

The 1MB Block Size Limit

No Limit

BIP 101, BIP 100, BIP 102, BIP 106, BIP ??

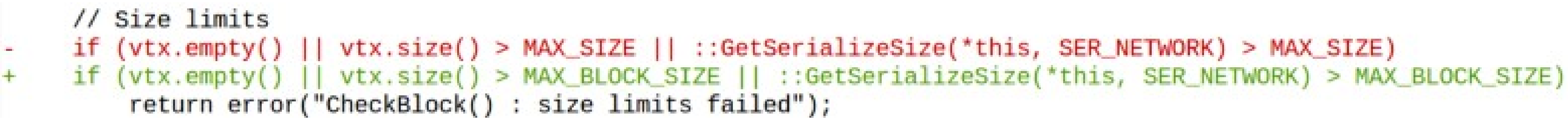
Segregated Witness

CLTV, CSV, Payment Channels & Lightning

Strategy for Bitcoin Wallets

1MB Block Size Limit

- 1MB block size limit enacted in Sep. 2010 by Satoshi. Originally just a MAX_SIZE limit of 32MB.
- Commit 172f006020965ae8763a0610845c051ed1e3b522
- No explanation given in commit message.
- If blocks are unlimited in size, theoretically, attacker could send large numbers of transactions to DOS attack network. Post-facto justification.



```
    // Size limits
-   if (vtx.empty() || vtx.size() > MAX_SIZE || ::GetSerializeSize(*this, SER_NETWORK) > MAX_SIZE)
+   if (vtx.empty() || vtx.size() > MAX_BLOCK_SIZE || ::GetSerializeSize(*this, SER_NETWORK) > MAX_BLOCK_SIZE)
        return error("CheckBlock() : size limits failed");
```

1MB Block Size Limit

- 1MB limits to 7 transactions per second for the smallest pubkeyhash transactions.
- By comparison, VISA handles ~4000 per second, which would require 500 MB blocks
- If every person in the world did 1 tx per day, that would require ~10 GB blocks
- 1MB blocks requires minimum 1.6 KB/s bandwidth
- 10GB blocks requires minimum 16 MB/s bandwidth

1MB Block Size Limit

- **Miners**: Want more transactions, but also want fees, and don't want to be bandwidthed-out by competition. Chinese miners have tougher time getting blocks in/out.
- **Users**: Want more transactions, don't care about block size if they don't want a node, care deeply if they do run a node.
- **Companies**: Want more transactions, willing to shoulder burden of running nodes, but causes centralization pressure if users can't.

1MB Block Size Limit

- **Hard Fork**: Requires everyone to agree to changes to protocol. What if some don't agree?
- **Soft Fork**: Doesn't require anyone to agree – old nodes continue to function like normal.
- **A max block size increase is a hard fork** – causes tremendous disagreement and dram, even if differences are subtle

1MB Block Size Limit

- Summary: **Everyone wants more transactions**. People do not agree about how.
- Series of proposals have been made. Four kinds:
  - **1) Increase by block size** by various means
  - **2) Segregated Witness**
  - **3) Off-Chain Decentralized** (payment channels)
  - **4) Off-Chain Centralized**
- Some can be implemented simultaneously.
- Outcome uncertain

No Limit

- Bitcoin did not originally have a limit.
- Peter R, “A Transaction Fee Market Exists Without A Block Size Limit”, https://scalingbitcoin.org/papers/feemarket.pdf
- Justus Ranvier series of blog posts: https://bitcoinism.liberty.me/economic-fallacies-and-the-block-size-limit-part-1-scarcity/

BIP 101

- By Gavin Andresen, Chief Scientist of Bitcoin Foundation
- Max block size: 8MB on Jan 11, 2016, then **double every two years**. Scales with Moore's Law.
- Implemented in **Bitcoin XT**, a fork of Bitcoin Core.
- Most popular “increase the block size” proposal. Most bitcoin APIs and wallets support this.
- Changes block version number to before hard forking. Some miner support, but enough at present to activate.
- Hostile reaction from some community members.

BIP 100

- By Jeff Garzik, Bitcoin Core developer, founder Bloq
- http://gtf.org/garzik/bitcoin/BIP100-blocksizechangeproposal.pdf
- Miners vote periodically on what the max block size should be – floor of middle 60% of votes is size.
- 32MB max data size remains.
- Popular amongst miners and some others.
- Not implemented.

BIP 102

- By Jeff Garzik, Bitcoin Core developer, founder Bloq
- One time increase to 2MB.
- Temporary solution. Would have to revisit the issue continuously.
- Easy to implement.

BIP 106

- “Dynamically Controlled Bitcoin Block Size Max Cap” by Upal Chakraborty
- https://github.com/bitcoin/bips/blob/master/bip-0106.mediawiki
- Double block size if blocks are over 90% full
- Halve block size if blocks are under 50% full
- Also includes logic that depends on miner fees
- Not great community traction. Not implemented.

BIP ?? by Pieter Wuille

- (“??” because it hasn't been assigned a BIP number)
- https://gist.github.com/sipa/c65665fc360ca7a176a6
- “Increase according to technological growth”
- Increase of 4.4% every ~97 days, or ~17.7% growth per year
- Designed to track technological increase in bandwidth
- Not much traction. (Not implemented?)

Segregated Witness

- Embed second Merkle root in Coinbase transactions that include signatures.
- All normal transactions become ANYONECANPAY.
- Effectively removes signatures from blocks, ~halving block size, and putting them in a new data structure.
- The only “block size increase” that can be accomplished with a **soft fork**, pleasing everyone.
- Also comes with an extra flag on scripts to allow future script language soft forks.
- Everyone likes this. Has an implementation. Not a long-term solution, but pretty good for right now.

Off-Chain Decentralized

- CHECKLOCKTIMEVERIFY and CHECKSEQUENCEVERIFY allow for secure payment channels:
  - Payer embeds one transaction on blockchain locked for a day, can be used as refund if things go wrong
  - Sends updated transaction to payee in small increments, sending more to payee with each update, and all change back to themselves
  - Allows tiny incremental payment off-chain. Settle on blockchain.
- Can set up network of trust-minimized payment channel providers. Most transactions go through network of payment channels and stay off chain, keeping on-chain fees minimal.
- Lightning Network is an example of a network of payment channels.

My Prediction

- Segregated Witness will be implemented soon. Stopgap.
- CLTV already implemented. CSV next. Then payment channels become secure. Can then run decentralized payment network layer on top. Wallets adapt ~2 years.
- Fee market develops during this time.
- Ultimately, fees become very high. Can uncontroversially agree to moderately raise block size.
- ...all this holds *unless* another implementation can sway the community soon, like Bitcoin XT or btcd.

What Wallets Should Do

- Implement segregated witness, CLTV, CSV, lightning network. Will require difficult re-architecture of software.
- 1) Turn on segregated witness, when possible.
- 2) Turn on lightning network, when possible.
- Do not assume blocks will increase in size any time soon.
- Do not assume 0 confirm transactions are valid.
- Do not assume 0 fee transactions will be confirmed.
- ...or, push for an alternative implementation with bigger blocks, causing painful hard fork, but no difficult software re-architectures.

Conclusion

- Bitcoin can't handle many transactions right now.
- Need bigger blocks or some other clever solution.
- Segregated witness will probably be implemented first. A variety of other advanced techniques will also be implemented, requiring wallet support.
- Long-term future unclear. Will probably involve innovative solutions, hard to predict. One step at a time.