This document updates the previous roadmap [1] of Dec 2015. The older statement endorsed a belief that "the community is ready to deliver on its shared vision that addresses the needs of the system while upholding its values".

That belief has not changed, but the shared vision has certainly grown sharper over the last 18 months. Below is a list of technologies which either increase Bitcoin's maximum tps rate ("capacity"), or which make it easier to process a higher volume of transactions ("scalability").

First, over the past 18 months, the technical community has completed a number of items [2] on the Dec 2015 roadmap. VersonBits (BIP 9) enables Bitcoin to handle multiple soft fork upgrades at once. Compact Blocks (BIP 152) allows for much faster block propagation, as does the FIBRE Network [3]. Check Sequence Verify (BIP 112) allows trading partners to mutually update an active transaction without writing it to the blockchain (this helps to enable the Lightning Network).

Second, Segregated Witness (BIP 141), which reorganizes data in blocks to handle signatures separately, has been completed and awaits activation (multiple BIPS). It is estimated to increase capacity by a factor of 2.2. It also improves scalability in many ways. First, SW includes a fee-policy which encourages users to minimize their impact on the UTXO set. Second, SW achieves linear scaling of sighash operations, which prevents the network from crashing when large transactions are broadcast. Third, SW provides an efficiency gain for everyone who is not verifying signatures, as these no longer need to be downloaded or stored. SegWit is an enabling technology for the Lightning Network, script versioning (specifically Schnorr signatures), and has a number of benefits which
are unrelated to capacity [4].

Third, the Lightning Network, which allows users to transact without broadcasting to the network, is complete [5, 6] and awaits the activation of SegWit. For those users who are able to make a single on-chain transaction, it is estimated to increase both capacity and scalability by a factor of ~1000 (although these capacity increases will vary with usage patterns). LN also greatly improves transaction speed and transaction privacy.

Fourth, Transaction Compression [7], observes that Bitcoin transaction serialization is not optimized for storage or network communication. If transactions were optimally compressed (as is possible today), this would improve scalability, but not capacity, by roughly 20%, and in some cases over 30%.

Fifth, Schnorr Signature Aggregation, which shrinks transactions by allowing many transactions to have a single shared signature, has been implemented [8] in draft form in libsecp256k1, and will likely be ready by Q4 of 2016. One analysis [9] suggests that signature aggregation would result in storage and bandwidth savings of at least 25%, which would therefore increase

scalability and capacity by a factor of 1.33. The relative savings are even greater for multisignature transactions.

Sixth, drivechain [10], which allows bitcoins to be temporarily offloaded to 'alternative' blockchain networks ("sidechains"), is currently under peer review and may be usable by end of 2017. Although it has no impact on scalability, it does allow users to opt-in to greater capacity, by moving their BTC to a new network (although, they will achieve less decentralization as a result). Individual drivechains may have different security tradeoffs (for example, a greater reliance on UTXO commitments, or MimbleWimble's shrinking block history) which may give them individually greater scalability than mainchain Bitcoin.

Finally, the capacity improvements outlined above may not be sufficient. If so, it may be necessary to use a hard fork to increase the blocksize (and blockweight, sigops, etc) by a moderate amount. Such an increase should take advantage of the existing research on hard forks, which is substantial [11]. Specifically, there is some consensus that Spoonnet [12] is the most attractive option for such a hardfork. There is currently no consensus on a hard fork date, but there is a rough consensus that one would require at least 6 months to coordinate effectively, which would place it in the year 2018 at earliest.

The above are only a small sample of current scaling technologies. And even an exhaustive list of scaling technologies, would itself only be a small sample of total Bitcoin innovation (which is proceeding at breakneck speed).

Signed,
<Names Here>

[1] https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-December/011865.html
[2] https://bitcoincore.org/en/2017/03/13/performance-optimizations-1/
[3] http://bluematt.bitcoin.ninja/2016/07/07/relay-networks/
[4] https://bitcoincore.org/en/2016/01/26/segwit-benefits/
[5] http://lightning.community/release/software/lnd/lightning/2017/05/03/litening/
[6] https://github.com/ACINQ/eclair
[7] https://people.xiph.org/~greg/compacted_txn.txt
[8]
https://github.com/ElementsProject/secp256k1-zkp/blob/d78f12b04ec3d9f5744cd4c51f20951106b9c41a/src/secp256k1.c#L592-L594
[9] https://bitcoincore.org/en/2017/03/23/schnorr-signature-aggregation/
[10] http://www.drivechain.info/
[11] https://bitcoinhardforkresearch.github.io/
[12] https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2017-February/013542.html