cducrest:

We can also recover liveness by stating that if no block is produced during n slots (due to not having the decryption key), the next block does not need to include a decryption key, and decrypted transactions are ignored.

How do you identify that the reason the block wasn’t produced was because decryption keys were missing and not for any other reason?

It also feels like it is fairly critical (for liveness) to have the number of missing slots before reorging out the block in question to be very low, and we would need the reorg to be at most

less deep than the most recent justified

block so we can maintain other guarantees. There is also discussion about moving the safe

block to pretty close to head (maybe not even a full block behind), in which case I would be very loath to have a condition under which a safe

block gets reorged out (but may be open to it in the safe

case, but not justified

case).