EE374 Blockchain Infrastructure **Stanford, Spring 2025**

Discussion Section #5

May 6, 2025

1. **Proof of Safety for Tendermint:**

   We have previously observed that when $n = 3f + 1$ and the number of (Byzantine) adversarial nodes is less than or equal to f, it is not possible for two distinct blocks proposed for the same round to be confirmed (except with negligible probability).

   We now turn our attention to blocks from different rounds. For contradiction, suppose two different blocks B_r and $B_{r'}$ proposed for rounds r and $r' > r$ are both confirmed. Then, $2f + 1$ nodes must have sent round-r pre-commits for B_r, and thus must have acquired a round r lock on block B_r. Similarly, $2f + 1$ nodes must have sent round-r' pre-commits for $B_{r'}$.

   By the bound on the number of adversarial nodes, at least one honest node (in fact, at least $f + 1$ honest nodes) must have sent round-r' pre-commits for $B_{r'}$. Then, these honest nodes must have observed $2f + 1$ round-r' pre-votes for $B_{r'}$. Now, by a quorum intersection argument, at least $f + 1$ nodes, i.e., at least one honest node v^h_1, must have acquired a round r lock on block B_r, yet sent a round-r' pre-vote for $B_{r'} \neq B_r$. Note that the honest node v^h_1 is allowed to do so, if (i) $B_{r'}$ came as part of a proposal $\langle \mathsf{Proposal}, r', vr, B_{r'} \rangle$, (ii) v^h_1 observed $2f + 1$ round-vr pre-votes for $B_{r'}$, and (iii) $vr > r$ (and of course, $vr < r'$). This is the temporary lock-release discussed in the class.

   The observations above implies that there must be at least $2f + 1$ round-vr pre-votes for $B_{r'} \neq B_r$, where $vr > r$. Again by a quorum intersection argument, at least $f + 1$ nodes, i.e., at least one honest node, must have acquired a round r lock on block B_r, yet sent a round-vr pre-vote for $B_{r'} \neq B_r$, despite the fact that $vr > r$. Repeating the temporary lock-release argument above (if necessary multiple times), we conclude that there must be a *first* round $vr^* > r$ such that at least $2f + 1$ nodes sent a round-vr^* pre-vote for $B_{r'} \neq B_r$. Finally, this implies at least $f + 1$ nodes, i.e., at least one honest node v^h_2, must have acquired a round r lock on block B_r, yet sent a round-vr^* pre-vote for $B_{r'} \neq B_r$, where $vr^* > r$. However, by definition of vr^*, v^h_2 could not have observed $2f+1$ round-vr pre-votes for $B_{r'}$ for any vr such that $r < vr < vr^*$. Therefore, v^h_2 must have dropped its round r lock on B_r for no reason, which is a protocol violation. As honest nodes do not violate the protocol rules, we have a contradiction, and two different blocks B_r and $B_{r'}$ proposed for different rounds cannot both be confirmed.

2. **Accountable safety implies safety under honesty assumptions:** Suppose a protocol satisfies accountable safety with resilience $f+1$, which means that if safety is violated, at least $f+1$ adversarial nodes can be identified as protocol violators via a cryptographic

proof (and no honest node is ever identified, except with negligible probability). Now, if the number of adversarial validators is bounded by f, the protocol must remain safe. We prove this by contradiction.

Suppose there are only f adversarial validators and the protocol is not safe. Then, when safety is violated, accountable safety requires at least $f + 1$ adversarial nodes to be identified as protocol violators. However, there are only f adversarial validators in total, contradiction!