APPENDIX

A. Definition

elected-fallback block: We refer to an fallback block B_f generated in view v with level 2 as an elected-fallback block, if the common-coin-flip(v) returns the index of the proposer p_l who generated B_f in the view v and if the <asynchronous-complete> for B_f exists in the first $n-f$ <asynchronous-complete> messages received. An elected-fallback block is committed same as a synchronously-committed block.

B. Proof of agreement

Theorem 1. *Let B and $\tilde{B}$ be two blocks with rank (v,r). Each of B and $\tilde{B}$ can be of type: (1) synchronous block which collects at least $n-f$ votes or (2) elected-fallback block or (3) level 1 fallback block which is a parent of an elected-fallback block. Then $\tilde{B}$ and B are the same.*

Proof. This holds directly from the block formation – if both B and $\tilde{B}$ has the same rank, then due to quorum intersection, there exists at least one node who voted for both blocks in the same rank, which is a contradiction to our assumption of non malicious nodes. □

Theorem 2. *Let B and $\tilde{B}$ be two adjacent blocks, then $\tilde{B}.r = B.r + 1$ and $\tilde{B}.v \geq B.v$.*

Proof. According to the algorithm, there are three instances where a new block is created.

- Case 1: when $isAsync$ = false and L_{vcur} creates a new synchronous block by extending the $block_{high}$ with rank (v,r). In this case, L_{vcur} creates a new block with round $r+1$. Hence the adjacent blocks have monotonically increasing round numbers.
- Case 2: when $isAsync$ = true and upon collecting $n-f$ <timeout> messages in view v. In this case, the replica selects the $block_{high}$ with the highest rank (v,r), and extends it by proposing a level 1 fallback block with round $r+1$. Hence the adjacent blocks have monotonically increasing round numbers.
- Case 3: when $isAsync$ = true and upon collecting $n-f$ <vote-async> messages for a level 1 fallback block. In this case, the replica extends the level 1 block by proposing a level 2 block with round $r+1$. Hence the adjacent blocks have monotonically increasing round numbers.

The view numbers are non decreasing according to the algorithm. Hence Theorem 2 holds. □

Theorem 3. *If a synchronous block B_c with rank (v,r) is committed, then all future blocks in view v will extend B_c.*

Proof. We prove this by contradiction.

Assume there is a committed block B_c with $B_c.r$ = r_c (hence all the blocks in the path from the genesis block to B_c are committed). Let block B_s with $B_s.r$ = r_s be the round r_s block such that B_s conflicts with B_c (B_s does not extend B_c). Without loss of generality, assume that $r_c < r_s$.

Let block B_f with $B_f.r$ = r_f be the first valid block formed in a round r_f such that $r_s \geq r_f > r_c$ and B_f is the first block from the path from genesis block to B_s that conflicts with B_c; for instance B_f could be B_s. L_{vcur} forms B_f by extending its $block_{high}$. Due to the minimality of B_f (B_f is the first block that conflicts with B_c), $block_{high}$ contain either B_c or a block that extends B_c. Since $block_{high}$ extends B_c, B_f extends B_c, thus we reach a contradiction. Hence no such B_f exists. Hence all the blocks created after B_c in the view v extend B_c. □

Theorem 4. *If a synchronous block B with rank (v, r) is committed, an elected-fallback block $\tilde{B}$ of the same view v will extend that block.*

Proof. We prove this by contradiction. Assume that a synchronous block B is committed in view v and an elected-fallback block $\tilde{B}$ does not extend B. Then, the parent level 1 block of $\tilde{B}$, $\tilde{B}_p$, also does not extend B.

To form the level 1 $\tilde{B}_p$, the replica collects $n-f$ <timeout> messages, each of them containing the $block_{high}$. If B is committed, by theorem 3, at least $n-f$ replicas should have set (and possibly sent) B or a block extending B as the $block_{high}$. Hence by intersection of the quorums $\tilde{B}_p$ extends B, thus we reach a contradiction. □

Theorem 5. *At most one level 2 fallback block from one proposer can be committed in a given view change.*

Proof. Assume by way of contradiction that 2 level 2 fallback blocks from two different proposers are committed in the same view. A level 2 fallback block B is committed in the fallback phase if the common-coin-flip(v) returns the proposer of B as the elected proposer. Since the common-coin-flip(v) outputs the same elected proposer across different replicas, this is a contradiction. Thus all level 2 fallback blocks committed during the same view are from the same proposer.

Assume now that the same proposer proposed two different level 2 fallback blocks. Since no replica can equivocate, this is absurd.

Thus at most one level 2 fallback block from one proposer can be committed in a given view change. □

Theorem 6. *Let B be a level 2 elected-fallback block that is committed, then all blocks proposed in the subsequent rounds extend B.*

Proof. We prove this by contradiction. Assume that level two elected-fallback block B is committed with rank (v, r) and block $\tilde{B}$ with rank ($\tilde{v}$, $\tilde{r}$) such that ($\tilde{v}$, $\tilde{r}$) $>$ (v, r) is the first block in the chain starting from B that does not extend B. $\tilde{B}$ can be formed in two occurrences: (1) $\tilde{B}$ is a synchronous block in the view $v+1$ or (2) $\tilde{B}$ is a level 1 fallback block with a view strictly greater than v. (we do not consider the case where $\tilde{B}$ is a level 2 elected-fallback block, because this directly follows from 1)

If B is committed, then from the algorithm construction it is clear that a majority of the replicas will set B as $block_{high}$. This is because, to send a <asynchronous-complete> message with B, a replica should collect at least $n-f$ <vote-async> messages. Hence, its guaranteed that if $\tilde{B}$ is formed in view v+1 as a synchronous block, then it will observe B as the $block_{high}$, thus we reach a contradiction.

In the second case, if $\tilde{B}$ is formed in a subsequent view, then it is guaranteed that the level 1 block will extend B by gathering from the <timeout> messages B as $block_{high}$ or a block extending B as the $block_{high}$, hence we reach a contradiction. □

Theorem 7. *There exists a single history of committed blocks.*

Proof. Assume by way of contradiction there are two different histories H_1 and H_2 of committed blocks. Then there is at least one block from H_1 that does not extend at least one block from H_2. This is a contradiction with theorems 3, 4 and 6. Hence there exists a single chain of committed blocks. □

Theorem 8. *For each committed replicated log position r, all replicas contain the same block.*

Proof. By theorem 2, the committed chain will have incrementally increasing round numbers. Hence for each round number (log position), there is a single committed entry, and by theorem 1, this entry is unique. This completes the proof. □

C. Proof of termination

Theorem 9. *If at least $n-f$ replicas enter the fallback phase of view v by setting $isAsync$ to true, then eventually they all exit the fallback phase and set $isAsync$ to false.*

Proof. If $n-f$ replicas enter the fallback path, then eventually all replicas (except for failed replicas) will enter the fallback path as there are less than $n-f$ replicas left on the synchronous path due to quorum intersection, so no progress can be made on the synchronous path and all replicas will timeout. As a result, at least $n-f$ correct replicas will broadcast their <timeout> message and all replicas will enter the fallback path.

Upon entering the fallback path, each replica creates a fallback block with level 1 and broadcasts it. Since we use perfect point-to-point links, eventually all the level 1 blocks sent by the $n-f$ correct replicas will be received by each replica in the fallback path. At least $n-f$ correct replicas will send them <vote-async> messages if the rank of the level 1 block is greater than the rank of the replica. To ensure liveness for the replicas that have a lower rank, the algorithm allows catching up, so that nodes will adopt whichever level 1 block which received $n-f$ <vote-async> arrives first. Upon receiving the first level 1 block with $n-f$ <vote-async> messages, each replica will send a level 2 fallback block, which will be eventually received by all the replicas in the fallback path. Since the level 2 block proposed by any block passes the rank test for receiving a <vote-async>, eventually at least $n-f$ level 2 blocks get $n-f$ <vote-async>. Hence, eventually at least $n-f$ replicas send the <asynchronous-complete> message, and exit the fallback path. □

Theorem 10. *With probability* p¿$\frac{1}{2}$*, at least one replica commits an elected-fallback block after exiting the fallback path.*

Proof. Let leader $L_{elected}$ be the output of the common-coin-flip(v). A replica commits a block during the fallback mode if the <asynchronous-complete> message from $L_{elected}$ is among the first $n - f$ <asynchronous-complete> messages received during the fallback mode, which happens with probability at least greater than $\frac{1}{2}$. Hence with probability no less than $\frac{1}{2}$, each replica commits a chain in a given fallback phase. □

Theorem 11. *A majority of replicas keep committing new blocks with high probability.*

Proof. We first prove this theorem for the basic case where all replicas start the protocol with $v = 0$. If at least $n - f$ replicas eventually enter the fallback path, by theorem 9, they eventually all exit the fallback path, and a new block is committed by at least one replica with probability no less than $\frac{1}{2}$. According to the asynchronous-complete step, all nodes who enter the fallback path enter view $v = 1$ after exiting the fallback path. If at least $n - f$ replicas never set $isAsync$ to true, this implies that the sequence of blocks produced in view 1 is infinite. By Theorem 2, the blocks have consecutive round numbers, and thus a majority replicas keep committing new blocks.

Now assume the theorem 11 is true for view $v = 0, ..., k-1$. Consider the case where at least $n - f$ replicas enter the view $v = k$. By the same argument for the $v = 0$ base case, $n - f$ replicas either all enter the fallback path commits a new block with $\frac{1}{2}$ probability, or keeps committing new blocks in view k. Therefore, by induction, a majority replicas keep committing new blocks with high probability. □

Theorem 12. *Each client command is eventually committed.*

Proof. If each replica repeatedly keeps proposing the client commands until they become committed, then eventually each client command gets committed according to theorem 11. □