1 Model

We consider a static set of n processes with known identities, communicating by reliable point-to-point channels, in a complete graph. Messages are uniquely identifiable.

Synchrony. The network is asynchronous. Processes may crash; at most f crashes occur.

Communication. Processes can exchange through a Reliable Broadcast (RB) primitive (defined below) which is invoked with the functions $\mathsf{RB\text{-}cast}(m)$ and $\mathsf{RB\text{-}received}(m)$. There exists a shared object called DenyList (DL) (defined below) that is interfaced with the functions $\mathsf{APPEND}(x)$, $\mathsf{PROVE}(x)$ and $\mathsf{READ}()$.

Notation. Let Π be the finite set of process identifiers and let $n \triangleq |\Pi|$. Two authorization subsets are $\Pi_M \subseteq \Pi$ (processes allowed to issue APPEND) and $\Pi_V \subseteq \Pi$ (processes allowed to issue PROVE). Indices $i, j \in \Pi$ refer to processes, and p_i denotes the process with identifier i. Let $\mathcal{M}$ denote the universe of uniquely identifiable messages, with $m \in \mathcal{M}$. Let $\mathcal{R} \subseteq \mathbb{N}$ be the set of round identifiers; we write $r \in \mathcal{R}$ for a round. We use the precedence relation $\prec$ for the DL linearization: $x \prec y$ means that operation x appears strictly before y in the linearized history of DL. For any finite set $A \subseteq \mathcal{M}$, $\mathsf{ordered}(A)$ returns a deterministic total order over A (e.g., lexicographic order on $(\mathit{senderId}, \mathit{messageId})$ or on message hashes). For any round $r \in \mathcal{R}$, define $\mathsf{Winners}_r \triangleq \{\, j \in \Pi \mid (j, \mathsf{prove}(r)) \prec \mathsf{APPEND}(r) \,\}$, i.e., the set of processes whose $\mathsf{PROVE}(r)$ appears before the first $\mathsf{APPEND}(r)$ in the DL linearization. We denoted by $\mathsf{PROVE}^{(j)}(r)$ or $\mathsf{APPEND}^{(j)}(r)$ the operation $\mathsf{PROVE}(r)$ or $\mathsf{APPEND}(r)$ invoked by process j.

2 Primitives

2.1 Reliable Broadcast (RB)

RB provides the following properties in the model.

- **Integrity**: Every message received was previously sent. $\forall p_i : \mathsf{RB\text{-}received}_i(m) \Rightarrow \exists p_j : \mathsf{RB\text{-}cast}_j(m)$.
- **No-duplicates**: No message is received more than once at any process.
- **Validity**: If a correct process broadcasts m, every correct process eventually receives m.

2.2 DenyList Object

We assume a synchronous DenyList (DL) object as in [?] with the following properties.

The DenyList object type supports three operations: APPEND, PROVE, and READ. These operations appear as if executed in a sequence Seq such that:

- **Termination.** A PROVE, an APPEND, or a READ operation invoked by a correct process always returns.
- **APPEND Validity.** The invocation of $\mathsf{APPEND}(x)$ by a process p is valid if:
  - $p \in \Pi_M \subseteq \Pi$; **and**
  - $x \in S$, where S is a predefined set.

Otherwise, the operation is invalid.

- **PROVE Validity.** If the invocation of a $op = \mathsf{PROVE}(x)$ by a correct process p is not valid, then:
  - $p \notin \Pi_V \subseteq \Pi$; **or**
  - A valid $\mathsf{APPEND}(x)$ appears before op in Seq.

  Otherwise, the operation is valid.

- **PROVE Anti-Flickering.** If the invocation of a operation $op = \mathsf{PROVE}(x)$ by a correct process $p \in \Pi_V$ is invalid, then any $\mathsf{PROVE}(x)$ operation that appears after op in Seq is invalid.

- **READ Validity.** The invocation of $op = \mathsf{READ}()$ by a process $p \in \pi_V$ returns the list of valid invocations of PROVE that appears before op in Seq along with the names of the processes that invoked each operation. item **Anonymity.** Let us assume the process p invokes a $\mathsf{PROVE}(v)$ operation. If the process p' invokes a $\mathsf{READ}()$ operation, then p' cannot learn the value v unless p leaks additional information.

We assume that $\Pi_M = \Pi_V = \Pi$ (all processes can invoke APPENDand PROVE).

3 Target Abstraction: Atomic Reliable Broadcast (ARB)

Processes export $\mathsf{AB\text{-}broadcast}(m)$ and $\mathsf{AB\text{-}deliver}(m)$. ARB requires total order:

$$\forall m_1, m_2,\ \forall p_i, p_j :\quad \mathsf{AB\text{-}deliver}_i(m_1) < \mathsf{AB\text{-}deliver}_i(m_2) \Rightarrow \mathsf{AB\text{-}deliver}_j(m_1) < \mathsf{AB\text{-}deliver}_j(m_2),$$

plus Integrity/No-duplicates/Validity (inherited from RB and the construction).

4 ARB over RB and DL

We present below an example of implementation of Atomic Reliable Broadcast (ARB) using a Reliable Broadcast (RB) primitive and a DenyList (DL) object according to the model and notations defined in Section 2.

4.1 Algorithm

Definition 1 (Closed round)**.** Given a DL linearization H, a round $r \in \mathcal{R}$ is *closed* in H iff H contains an operation $\mathsf{APPEND}(r)$. Equivalently, there exists a time after which every $\mathsf{PROVE}(r)$ is invalid in H.

4.1.1 Variables

Each process p_i maintains:

$\mathsf{received} \leftarrow \emptyset$ ▷ Messages received via RB but not yet delivered
$\mathsf{delivered} \leftarrow \emptyset$ ▷ Messages already delivered
$\mathsf{prop}[r][j] \leftarrow \bot,\ \forall r, j$ ▷ Proposal from process j for round r
$\mathsf{current} \leftarrow 0$

DenyList. The DLis initialized empty. We assume $\Pi_M = \Pi_V = \Pi$ (all processes can invoke APPENDand PROVE).

déjà def.

4.1.2 Handlers and Procedures

Algorithm A RB handler (at process p_i)

```
function RBReceived(S, r, j)
    received ← received ∪ {S}
    prop[r][j] ← S                                   ▷ Record sender j's proposal S for round r
end function
```

Algorithm B AB-broadcast(m) (at process p_i)

```
function ABBroadcast(m)
    P ← READ()                         ▷ Fetch latest DLstate to learn recent PROVE operations
    r_max ← max({r' : ∃j, (j, PROVE(r')) ∈ P})                       ▷ Pick current open round
    S ← (received \ delivered) ∪ {m}          ▷ Propose all pending messages plus the new m

    for each r ∈ {r_max, r_max + 1, · · · } do
        RB-cast(S, r, i); PROVE(r); APPEND(r);
        P ← READ()                                               ▷ Refresh local view of DL
        if (((i, prove(r)) ∈ P ∨ (∃j, r' : (j, prove(r')) ∈ P ∧ m ∈ prop[r'][j]))) then
            break                          ▷ Exit loop once m is included in some closed round
        end if
    end for
end function
```

r ≥ rmax
repeat
until ?

encoder en (j, r) ?

Algorithm C AB-deliver() at process p_i

```
function ABdeliver
    r ← current
    P ← READ()
    if ∀j : (j, prove(r)) ∉ P then
        return ⊥
    end if
    APPEND(r); P ← READ()
    W_r ← {j : (j, prove(r)) ∈ P}
    if ∃j ∈ W_r, prop[r][j] = ⊥ then
        return ⊥
    end if
    M_r ← ⋃_{j∈W_r} prop[r][j]
    m ← ordered(M_r \ delivered)[0]      ▷ Set m as the smaller message not already delivered
    delivered ← delivered ∪ {m}
    if M_r \ delivered = ∅ then          ▷ Check if all messages from round r have been delivered
        current ← current + 1
    end if
    return m
end function
```

4.2 Correctness

Lemma 1 (Stable round closure)**.** *If a round r is closed, then there exists a linearization point t_0 of APPEND(r) in the DL, and from that point on, no PROVE(r) can be valid. Once closed, a round never becomes open again.*

Proof. By Definition 1, some APPEND(r) occurs in the linearization H.
H is a total order of operations, the set of APPEND(r) operations is totally ordered, and hence there exists a smallest APPEND(r) in H. We denote this operation APPEND$^{(\star)}(r)$ and t_0 its linearization point.
By the validity property of DL, a PROVE(r) is valid iff PROVE$(r) \prec$ APPEND$^{(\star)}(r)$. Thus, after t_0, no PROVE(r) can be valid.
H is a immutable grow-only history, and hence once closed, a round never becomes open again.
Hence there exists a linearization point t_0 of APPEND(r) in the DL, and from that point on, no PROVE(r) can be valid and the closure is stable. □

Definition 2 (First APPEND)**.** Given a DL linearization H, for any closed round $r \in \mathcal{R}$, we denote by APPEND$^{(\star)}(r)$ the earliest APPEND(r) in H.

Lemma 2 (Across rounds)**.** *If there exists a r such that r is closed, $\forall r'$ such that $r' < r$, r' is also closed.*

Proof. Base. For a closed round $k = 0$, the set $\{k' \in \mathcal{R},\ k' < k\}$ is empty, hence the lemma is true.

Induction. Assume the lemma is true for round $k \geq 0$, we prove it for round $k + 1$.

Assume $k + 1$ is closed and let APPEND$^{(\star)}(k + 1)$ be the earliest APPEND$(k + 1)$ in the DL linearization H. By Lemma 1, after an APPEND(k) is in H, any later PROVE(k) is rejected also, a process's program order is preserved in H.

There are two possibilities for where APPEND$^{(\star)}(k + 1)$ is invoked.

- **Case (B6) :** Some process $p^\star$ executes the loop (lines B5–B11) and invokes $\mathsf{APPEND}^{(\star)}(k+1)$ at line B6. Immediately before line B6, line B5 sets $r \leftarrow r+1$, so the previous loop iteration (if any) targeted k. We consider two sub-cases.
  - *(i) $p^\star$ is not in its first loop iteration.* In the previous iteration, $p^\star$ executed $\mathsf{PROVE}^{(\star)}(k)$ at B6, followed (in program order) by $\mathsf{APPEND}^{(\star)}(k)$. If round k wasn't closed when $p^\star$ execute $\mathsf{PROVE}^{(\star)}(k)$ at B9, then the condition at B8 would be true hence the tuple $(p^\star, \mathsf{prove}(k))$ should be visible in P which implies that $p^\star$ should leave the loop at round k, contradicting the assumption that $p^\star$ is now executing another iteration. Since the tuple is not visible, the $\mathsf{PROVE}^{(\star)}(k)$ was rejected by the DL which implies by definition an $\mathsf{APPEND}(k)$ already exists in H. Thus in this case k is closed.
  - *(ii) $p^\star$ is in its first loop iteration.* To compute the value r_{max}, $p^\star$ must have observed one or many $(\_, \mathsf{prove}(k+1))$ in P at B2/B3, issued by some processes (possibly different from $p^\star$). Let's call p_1 the issuer of the first $\mathsf{PROVE}^{(1)}(k+1)$ in the linearization H. When p_1 executed $P \leftarrow \mathsf{READ}()$ at B2 and compute r_{max} at B3, he observed no tuple $(\_, \mathsf{prove}(k+1))$ in P because he's the issuer of the first one. So when p_1 executed the loop (B5–B11), he run it for the round k, didn't seen any $(1, \mathsf{prove}(k))$ in P at B8, and then executed the first $\mathsf{PROVE}^{(1)}(k+1)$ at B6 in a second iteration.
    If round k wasn't closed when p_1 execute $\mathsf{PROVE}^{(1)}(k)$ at B6, then the condition at B8 should be true which implies that p_1 sould leave the loop at round k, contradicting the assumption that p_1 is now executing $\mathsf{PROVE}^{(1)}(r+1)$. In this case k is closed.
- **Case (C8) :** Some process invokes $\mathsf{APPEND}(k+1)$ at C8. Line C8 is guarded by the presence of $\mathsf{PROVE}(next)$ in P with $next = k+1$ (C5). Moreover, the local pointer $next$ grow by increment of 1 and only advances after finishing the current round (C17), so if a process can reach $next = k+1$ it implies that he has completed round k, which includes closing k at C8 when $\mathsf{PROVE}(k)$ is observed. Hence $\mathsf{APPEND}^\star(k+1)$ implies a prior $\mathsf{APPEND}(k)$ in H, so k is closed.

In all cases, $k+1$ closed implie k closed. By induction on k, if the lemme is true for a closed k then it is true for a closed $k+1$. Therefore, the lemma is true for all closed rounds r. □

Definition 3 (Winner Invariant)**.** For any closed round r, define

$$\mathsf{Winners}_r \triangleq \{j : \mathsf{PROVE}^{(j)}(r) \prec \mathsf{APPEND}^\star(r)\}$$

as the unique set of winners of round r.

Lemma 3 (Invariant view of closure)**.** *For any closed round r, all correct processes eventually observe the same set of valid tuples $(\_, \mathsf{prove}(r))$ in their DLview.*

Proof. Let's take a closed round r. By Definition 2, there exists a unique earliest $\mathsf{APPEND}(r)$ in the DL linearization, denoted $\mathsf{APPEND}^\star(r)$.

Consider any correct process p that invokes $\mathsf{READ}()$ after $\mathsf{APPEND}^\star(r)$ in the DL linearization. Since $\mathsf{APPEND}^\star(r)$ invalidates all subsequent $\mathsf{PROVE}(r)$, the set of valid tuples $(\_, \mathsf{prove}(r))$ observed by any correct process after $\mathsf{APPEND}^\star(r)$ is fixed and identical across all correct processes.

Therefore, for any closed round r, all correct processes eventually observe the same set of valid tuples $(\_, \mathsf{prove}(r))$ in their DLview. □

Lemma 4 (Well-defined winners)**.** *For any correct process and round r, if the process computes W_r at line C9, then :*

- $\mathsf{Winners}_r$ *is defined;*
- *the computed W_r is exactly* $\mathsf{Winners}_r$*.*

Proof. Let take a correct process p_i that reach line C9 to compute W_r.
By program order, p_i must have executed $\mathsf{APPEND}^{(i)}(r)$ at C8 before, which implies by Definition 1 that round r is closed. So by Definition 3, $\mathsf{Winners}_r$ is defined.
By Lemma 3, all correct processes eventually observe the same set of valid tuples $(\_, \mathsf{prove}(r))$ in their DLview. Hence, when p_i executes the $\mathsf{READ}()$ at C8 after the $\mathsf{APPEND}^{(i)}(r)$, it observes a set P that includes all valid tuples $(\_, \mathsf{prove}(r))$ such that

$$W_r = \{j : (j, \mathsf{prove}(r)) \in P\} = \{j : \mathsf{PROVE}^{(j)}(r) \prec \mathsf{APPEND}^{\star}(r)\} = \mathsf{Winners}_r$$

□

Lemma 5 (No APPEND without PROVE)**.** *If some process invokes $\mathsf{APPEND}(r)$, then at least a process must have previously invoked $\mathsf{PROVE}(r)$.*

Proof. Consider the round r such that some process invokes $\mathsf{APPEND}(r)$. There are two possible cases

- **Case (B6) :** There exists a process $p^\star$ who's the issuer of the earliest $\mathsf{APPEND}^{(\star)}(r)$ in the DL linearization H. By program order, $p^\star$ must have previously invoked $\mathsf{PROVE}^{(\star)}(r)$ before invoking $\mathsf{APPEND}^{(\star)}(r)$ at B6. In this case, there is at least one $\mathsf{PROVE}(r)$ valid in H issued by a correct process before $\mathsf{APPEND}^{(\star)}(r)$.
- **Case (C8) :** There exist a process $p^\star$ invokes $\mathsf{APPEND}^{(\star)}(r)$ at C8. Line C8 is guarded by the condition at C5, which ensures that p observed some $(\_, \mathsf{prove}(r))$ in P. In this case, there is at least one $\mathsf{PROVE}(r)$ valid in H issued by some process before $\mathsf{APPEND}^{(\star)}(r)$.

In both cases, if some process invokes $\mathsf{APPEND}(r)$, then some process must have previously invoked $\mathsf{PROVE}(r)$. □

Lemma 6 (No empty winners)**.** *Let r be a round, if $\mathsf{Winners}_r$ is defined, then* $\mathsf{Winners}_r \neq \emptyset$*.*

Proof. If $\mathsf{Winners}_r$ is defined, then by Definition 3, round r is closed. By Definition 1, some $\mathsf{APPEND}(r)$ occurs in the DL linearization.
By Lemma 5, at least a process must have invoked a valid $\mathsf{PROVE}(r)$ before $\mathsf{APPEND}^{(\star)}(r)$. Hence, there exists at least one j such that $\{j : \mathsf{PROVE}^{(j)}(r) \prec \mathsf{APPEND}^{\star}(r)\}$, so $\mathsf{Winners}_r \neq \emptyset$. □

Lemma 7 (Winners must propose)**.** *For any closed round r, $\forall j \in$ $\mathsf{Winners}_r$, process j must have invoked a $\mathsf{RB\text{-}cast}(S^{(j)}, r, j)$*

Proof. Fix a closed round r. By Definition 3, for any $j \in \mathsf{Winners}_r$, there exist a valid $\mathsf{PROVE}^{(j)}(r)$ such that $\mathsf{PROVE}^{(j)}(r) \prec \mathsf{APPEND}^{\star}(r)$ in the DL linearization. By program order, if j invoked a valid $\mathsf{PROVE}^{(j)}(r)$ at line B6 he must have invoked $\mathsf{RB\text{-}cast}(S^{(j)}, r, j)$ directly before. □

Definition 4 (Messages invariant)**.** For any closed round r and any correct process p_i such that $\forall j \in \mathsf{Winners}_r : prop^{[i)}[r][j] \neq \bot$, define

$$\mathsf{Messages}_r \triangleq \bigcup_{j \in \mathsf{Winners}_r} \mathsf{prop}^{(i)}[r][j]$$

as the unique set of messages proposed by the winners of round r.

Lemma 8 (Non-empty winners proposal)**.** *For any closed round r, $\forall j \in \mathsf{Winners}_r$, for any correct process p_i, eventually $\mathsf{prop}^{(i)}[r][j] \neq \bot$.*

Proof. Fix a closed round r. By Definition 3, for any $j \in \mathsf{Winners}_r$, there exist a valid $\mathsf{PROVE}^{(j)}(r)$ such that $\mathsf{PROVE}^{(j)}(r) \prec \mathsf{APPEND}^{\star}(r)$ in the DL linearization. By Lemma 7, j must have invoked $\mathsf{RB\text{-}cast}(S^{(j)}, r, j)$.

Let take a process p_i, by RB *Validity*, every correct process eventually receives j's RB message for round r, which sets $\mathsf{prop}[r][j]$ to a non-$\bot$ value at line A3. □

Lemma 9 (Eventual proposal closure)**.** *If a correct process p_i define M_r at line C13, then for every $j \in \mathsf{Winners}_r$, $\mathsf{prop}^{(i)}[r][j] \neq \bot$.*

Proof. Let take a correct process p_i that computes M_r at line C13. By Lemma 4, p_i computes the unique winner set $\mathsf{Winners}_r$.

By Lemma 6, $\mathsf{Winners}_r \neq \emptyset$. The instruction at line C13 where p_i computes M_r is guarded by the condition at C10, which ensures that p_i has received all RB messages from every winner $j \in \mathsf{Winners}_r$. Hence, when p_i computes $M_r = \bigcup_{j \in \mathsf{Winners}_r} \mathsf{prop}^{(i)}[r][j]$, we have $\mathsf{prop}^{(i)}[r][j] \neq \bot$ for all $j \in \mathsf{Winners}_r$. □

Lemma 10 (Unique proposal per sender per round)**.** *For any round r and any process p_i, p_i invokes at most one $\mathsf{RB\text{-}cast}(S, r, i)$.*

Proof. By program order, any process p_i invokes $\mathsf{RB\text{-}cast}(S, r, i)$ at line B6 must be in the loop B5–B11. No matter the number of iterations of the loop, line B5 always uses the current value of r which is incremented by 1 at each turn. Hence, in any execution, any process p_i invokes $\mathsf{RB\text{-}cast}(S, r, j)$ at most once for any round r. □

Lemma 11 (Proposal convergence)**.** *For any round r, for any correct processes p_i that define M_r at line C13, we have*

$$M_r^{(i)} = \mathsf{Messages}_r$$

Proof. Let take a correct process p_i that define M_r at line C13. That implies that p_i has defined W_r at line C8. It implies that, by Lemma 4, r is closed and $W_r = \mathsf{Winners}_r$.
By Lemma 9, for every $j \in \mathsf{Winners}_r$, $\mathsf{prop}^{(i)}[r][j] \neq \bot$. By Lemma 10, each winner j invokes at most one $\mathsf{RB\text{-}cast}(S^{(j)}, r, j)$, so $\mathsf{prop}^{(i)}[r][j] = S^{(j)}$ is uniquely defined. Hence, when p_i computes

$$M_r^{(i)} = \bigcup_{j \in \mathsf{Winners}_r} \mathsf{prop}^{(i)}[r][j] = \bigcup_{j \in \mathsf{Winners}_r} S^{(j)} = \mathsf{Messages}_r.$$

□

Lemma 12 (Inclusion)**.** *If some correct process invokes $\mathsf{AB\text{-}broadcast}(m)$, then there exist a round r and a process $j \in \mathsf{Winners}_r$ such that p_j invokes*

$$\mathsf{RB\text{-}cast}(S, r, j) \quad \text{with} \quad m \in S.$$

Proof. Fix a correct process p_i that invokes $\mathsf{AB\text{-}broadcast}(m)$ and eventually exits the loop (B5–B11) at some round r. There are two possible cases.

- **Case 1:** p_i exits the loop because $(i, \mathsf{prove}(r)) \in P$. In this case, by Definition 3, p_i is a winner in round r. By program order, p_i must have invoked $\mathsf{RB\text{-}cast}(S, r, i)$ at B6 before invoking $\mathsf{PROVE}^{(i)}(r)$ at B7. By line B4, $m \in S$. Hence there exist a closed round r and a correct process $j = i \in \mathsf{Winners}_r$ such that j invokes $\mathsf{RB\text{-}cast}(S, r, j)$ with $m \in S$.
- **Case 2:** p_i exits the loop because $\exists j, r' : (j, \mathsf{prove}(r')) \in P \wedge m \in \mathsf{prop}[r'][j]$. In this case, by Lemma 7 and Lemma 10 j must have invoked a unique $\mathsf{RB\text{-}cast}(S, r', j)$. Which set $\mathsf{prop}^{(i)}[r'][j] = S$ with $m \in S$.

In both cases, if some correct process invokes $\mathsf{AB\text{-}broadcast}(m)$, then there exist a round r and a correct process $j \in \mathsf{Winners}_r$ such that j invokes

$$\mathsf{RB\text{-}cast}(S, r, j) \quad \text{with} \quad m \in S.$$

□

Lemma 13 (Broadcast Termination)**.** *If a correct process invokes $\mathsf{AB\text{-}broadcast}(m)$, then he eventually exit the function and returns.*

Proof. Let a correct process p_i that invokes $\mathsf{AB\text{-}broadcast}(m)$. The lemma is true if $\exists r_1$ such that $r_1 \geq r_{max}$ and if $(i, \mathsf{prove}(r_1)) \in P$; or if $\exists r_2$ such that $r_2 \geq r_{max}$ and if $\exists j : (j, \mathsf{prove}(r_2)) \in P \wedge m \in \mathsf{prop}[r_2][j]$ (like guarded at B8).

Let admit that there exists no round r_1 such that p_i invokes a valid $\mathsf{PROVE}(r_1)$. In this case p_i invokes infinitely many $\mathsf{RB\text{-}cast}(S, \_, i)$ at B6 with $m \in S$ (line B4).
The assumption that no $\mathsf{PROVE}(r_1)$ invoked by p is valid implies by DL *Validity* that for every round $r' \geq r_{max}$, there exists at least one $\mathsf{APPEND}(r')$ in the DL linearization, hence by Lemma 6 for every possible round r' there at least a winner. Because there is an infinite number of rounds, and a finite number of processes, there exists at least a correct process p_k that invokes infinitely many valid $\mathsf{PROVE}(r')$ and by extension infinitely many $\mathsf{AB\text{-}broadcast}(\_)$. By RB *Validity*, p_k eventually receives p_i 's RB messages. Let call t_0 the time when p_k receives p_i 's RB message.
At t_0, p_k execute Algorithm A and do $\mathsf{received} \leftarrow \mathsf{received} \cup \{S\}$ with $m \in S$ (line A2). For the first invocation of $\mathsf{AB\text{-}broadcast}(\_)$ by p_k after the execution of Algorithm A, p_k must include m in his proposal S at line B4 (because m is pending in j's $\mathsf{received} \setminus \mathsf{delivered}$ set). There exists a minimum round r_2 such that $p_k \in \mathsf{Winners}_{r_2}$ after t_0. By Lemma 8, eventually $\mathsf{prop}^{(i)}[r_2][k] \neq \bot$. By Lemma 10, $\mathsf{prop}^{(i)}[r_2][k]$ is uniquely defined as the set S proposed by p_k at B6, which by Lemma 12 includes m. Hence eventually $m \in \mathsf{prop}^{(i)}[r_2][k]$ and $k \in \mathsf{Winners}_{r_2}$.

So if p_i is a winner he cover the condition $(i, \mathsf{prove}(r_1)) \in P$. And we show that if the first condition is never satisfied, the second one will eventually be satisfied. Hence either the first or the second condition will eventually be satisfied, and p_i eventually exits the loop and returns from $\mathsf{AB\text{-}broadcast}(m)$. □

Lemma 14 (Validity)**.** *If a correct process p invokes $\mathsf{AB\text{-}broadcast}(m)$, then every correct process that invokes a infinitely often times $\mathsf{AB\text{-}deliver}()$ eventually delivers m.*

Proof. Let p_i a correct process that invokes $\mathsf{AB\text{-}broadcast}(m)$ and p_q a correct process that infinitely invokes $\mathsf{AB\text{-}deliver}()$. By Lemma 12, there exist a closed round r and a correct process $j \in \mathsf{Winners}_r$ such that p_j invokes

$$\mathsf{RB\text{-}cast}(S, r, j) \quad \text{with} \quad m \in S.$$

By Lemma 9, when p_j computes M_r at line C13, $\mathsf{prop}[r][j]$ is non-$\bot$ because $j \in \mathsf{Winners}_r$. By Lemma 10, p_j invokes at most one $\mathsf{RB\text{-}cast}(S, r, j)$, so $\mathsf{prop}[r][j]$ is uniquely defined. Hence, when p_j computes

$$M_r = \bigcup_{k \in \mathsf{Winners}_r} \mathsf{prop}[r][k],$$

we have $m \in \mathsf{prop}[r][j] = S$, so $m \in M_r$. By Lemma 11, M_r is invariant so each computation of M_r by any correct process that defines it includes m. At each invocation of $\mathsf{AB\text{-}deliver}()$ which deliver m', m' is add to $\mathsf{delivered}$ until $M_r \subseteq \mathsf{delivered}$. Once this append we're assured that there exist an invocation of $\mathsf{AB\text{-}deliver}()$ which return m. Hence m is well delivered. □

Lemma 15 (No duplication)**.** *No correct process delivers the same message more than once.*

Proof. Let consider two invokations of $\mathsf{AB\text{-}deliver}()$ made by the same correct process which returns m. Let call these two invocations respectively $\mathsf{AB\text{-}deliver}^{(A)}()$ and $\mathsf{AB\text{-}deliver}^{(B)}()$.

When $\mathsf{AB\text{-}deliver}^{(A)}()$ occur, by program order and because it reach line C19 to return m, the process must have add m to $\mathsf{delivered}$. Hence when $\mathsf{AB\text{-}deliver}^{(B)}()$ reach line C14 to extract the next message to deliver, it can't be m because $m \notin (M_r \setminus \{..., m, ...\})$. So a $\mathsf{AB\text{-}deliver}^{(B)}()$ which deliver m can't occur. □

Lemma 16 (Total order)**.** *For any two messages m_1 and m_2 delivered by correct processes, if a correct process p_i delivers m_1 before m_2, then any correct process p_j that delivers both m_1 and m_2 delivers m_1 before m_2.*

Proof. Consider any correct process that delivers both m_1 and m_2. By Lemma 14, there exist closed rounds r'_1 and r'_2 and correct processes $k_1 \in \mathsf{Winners}_{r'_1}$ and $k_2 \in \mathsf{Winners}_{r'_2}$ such that

$$\mathsf{RB\text{-}cast}(S_1, r'_1, k_1) \quad \text{with} \quad m_1 \in S_1,$$

$$\mathsf{RB\text{-}cast}(S_2, r'_2, k_2) \quad \text{with} \quad m_2 \in S_2.$$

Let consider three cases :

- **Case 1:** $r_1 < r_2$. By program order, any correct process must have waited to append in $\mathsf{delivered}$ every messages in M_{r_1} (which contains m_1) to increment $\mathsf{current}$ and eventually set $\mathsf{current} = r_2$ to compute M_{r_2} and then invoke the $\mathsf{AB\text{-}deliver}()$ that returns m_2. Hence, for any correct process that delivers both m_1 and m_2, it delivers m_1 before m_2.

- **Case 2:** $r_1 = r_2$. By Lemma 11, any correct process that computes M_{r_1} at line C13 computes the same set of messages $\mathsf{Messages}_{r_1}$. By line C14 the messages are pull in a deterministic order defined by $\mathsf{ordered}(\_)$. Hence, for any correct process that delivers both m_1 and m_2, it delivers m_1 and m_2 in the deterministic order defined by $\mathsf{ordered}(\_)$.

In all possible cases, any correct process that delivers both m_1 and m_2 delivers m_1 and m_2 in the same order. □

Lemma 17 (Fifo Order)**.** *For any two messages m_1 and m_2 broadcast by the same correct process p_i, if p_i invokes $\mathsf{AB\text{-}broadcast}(m_1)$ before $\mathsf{AB\text{-}broadcast}(m_2)$, then any correct process p_j that delivers both m_1 and m_2 delivers m_1 before m_2.*

Proof. Let take two messages m_1 and m_2 broadcast by the same correct process p_i, with p_i invoking AB-broadcast(m_1) before AB-broadcast(m_2). By Lemma 14, there exist closed rounds r_1 and r_2 and correct processes $k_1 \in \mathsf{Winners}_{r_1}$ and $k_2 \in \mathsf{Winners}_{r_2}$ such that

$$\mathsf{RB\text{-}cast}(S_1, r_1, k_1) \quad \text{with} \quad m_1 \in S_1,$$

$$\mathsf{RB\text{-}cast}(S_2, r_2, k_2) \quad \text{with} \quad m_2 \in S_2.$$

By program order, p_i must have invoked RB-cast(S_1, r_1, i) before RB-cast(S_2, r_2, i). By Lemma 10, any process invokes at most one RB-cast(S, r, i) per round, hence $r_1 < r_2$. By Lemma 16, any correct process that delivers both m_1 and m_2 delivers them in a deterministic order.

In all possible cases, any correct process that delivers both m_1 and m_2 delivers m_1 before m_2. □

Theorem 18 (FIFO-ARB)**.** *Under the assumed DLsynchrony and RB reliability, the algorithm implements FIFO Atomic Reliable Broadcast.*

Proof. We show that the algorithm satisfies the properties of FIFO Atomic Reliable Broadcast under the assumed DLsynchrony and RB reliability.

First, by Lemma 13, if a correct process invokes AB-broadcast(m), then it eventually returns from this invocation. Moreover, Lemma 14 states that if a correct process invokes AB-broadcast(m), then every correct process that invokes AB-deliver() infinitely often eventually delivers m. This gives the usual Validity property of ARB.

Concerning Integrity and No-duplicates, the construction only ever delivers messages that have been obtained from the underlying RB primitive. By the Integrity property of RB, every such message was previously RB-castby some process, so no spurious messages are delivered. In addition, Lemma 15 states that no correct process delivers the same message more than once. Together, these arguments yield the Integrity and No-duplicates properties required by ARB.

For the ordering guarantees, Lemma 16 shows that for any two messages m_1 and m_2 delivered by correct processes, every correct process that delivers both m_1 and m_2 delivers them in the same order. Hence all correct processes share a common total order on delivered messages. Furthermore, Lemma 17 states that for any two messages m_1 and m_2 broadcast by the same correct process, any correct process that delivers both messages delivers m_1 before m_2 whenever m_1 was broadcast before m_2. Thus the global total order extends the per-sender FIFO order of AB-broadcast.

All the above lemmas are proved under the assumptions that DLsatisfies the required synchrony properties and that the underlying primitive is a Reliable Broadcast (RB) with Integrity, No-duplicates and Validity. Therefore, under these assumptions, the algorithm satisfies Validity, Integrity/No-duplicates, total order and per-sender FIFO order, and hence implements FIFO Atomic Reliable Broadcast, as claimed. □

4.3 Reciprocity

So far, we assumed the existence of a synchronous DenyList (DL) object and showed how to upgrade a Reliable Broadcast (RB) primitive into FIFO Atomic Reliable Broadcast (ARB). We now briefly argue that, conversely, an ARB primitive is strong enough to implement a synchronous DLobject (ignoring the anonymity property).

DenyList as a deterministic state machine. Without anonymity, the DLspecification defines a deterministic abstract object: given a sequence Seq of operations APPEND(x), PROVE(x), and READ(), the resulting sequence of return values and the evolution of the abstract state (set of appended elements, history of operations) are uniquely determined.

State machine replication over ARB. Assume a system that exports a FIFO-ARB primitive with the guarantees that if a correct process invokes AB-broadcast(m), then every correct process eventually AB-deliver(m) and the invocation eventually returns. Following the classical *state machine replication* approach such as described in Schneider [1], we can implement a fault-tolerant service by ensuring the following properties:

> **Agreement.** Every nonfaulty state machine replica receives every request.
> **Order.** Every nonfaulty state machine replica processes the requests it receives in the same relative order.

Which are cover by our FIFO-ARB specification.

Correctness.

Theorem 19 (From ARB to synchronous DL). *In an asynchronous message-passing system with crash failures, assume a FIFO Atomic Reliable Broadcast primitive with Integrity, No-duplicates, Validity, and the liveness of AB-broadcast. Then, ignoring anonymity, there exists an implementation of a synchronous DenyList object that satisfies the Termination, Validity, and Anti-flickering properties.*

Proof. Because the DLobject is deterministic, all correct processes see the same sequence of operations and compute the same sequence of states and return values. We obtain:

- **Termination.** The liveness of ARB ensures that each AB-broadcast invocation by a correct process eventually returns, and the corresponding operation is eventually delivered and applied at all correct processes. Thus every APPEND, PROVE, and READ operation invoked by a correct process eventually returns.

- **APPEND/PROVE/READ Validity.** The local code that forms AB-broadcastrequests can achieve the same preconditions as in the abstract DLspecification (e.g., $p \in \Pi_M$, $x \in S$ for APPEND(x)). Once an operation is delivered, its effect and return value are exactly those of the sequential DLspecification applied in the common order.

- **PROVE Anti-Flickering.** In the sequential DLspecification, once an element x has been appended, all subsequent PROVE(x) are invalid forever. Since all replicas apply operations in the same order, this property holds in every execution of the replicated implementation: after the first linearization point of APPEND(x), no later PROVE(x) can return "valid" at any correct process.

Formally, we can describe the DLobject with the state machine approach for crash-fault, asynchronous message-passing systems with a total order broadcast layer [1]. □

4.3.1 Example executions

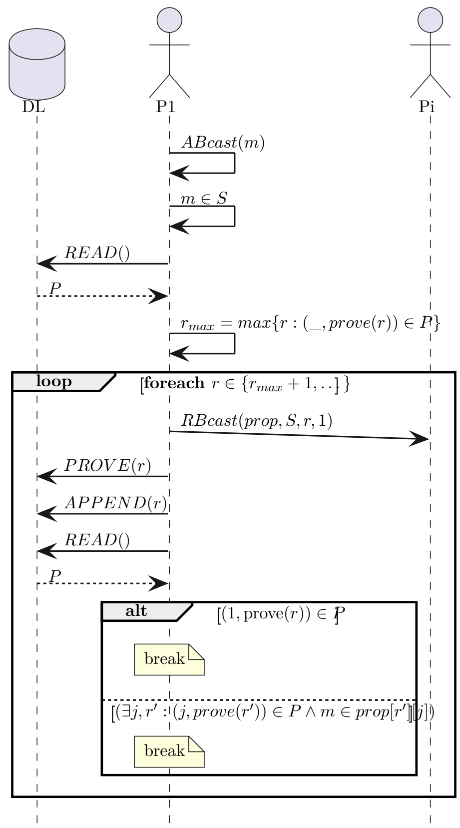

Figure 1: Example execution of the ARB algorithm in a non-BFT setting

à détailler

5 BFT-ARB over RB and DL

5.1 Model extension

We consider a static set of n processes with known identities, communicating by reliable point-to-point channels, in a complete graph. Messages are uniquely identifiable.

Synchrony. The network is asynchronous. Processes may crash or be byzantine.

Communication. Processes can exchange through a Reliable Broadcast (RB) object (defined below) which is invoked with the functions RB-cast(m) and RB-received(). There exists n shared object called DenyList (DL) (defined below) that is interfaced with the functions APPEND(x), PROVE(x) and READ().

Byzantine behaviour A process is said to exhibit Byzantine behaviour if it deviates arbitrarily from the prescribed algorithm. Such deviations may, for instance, consist in invoking primitives (RB-cast, APPEND, PROVE, etc.) with invalid inputs or inputs crafted maliciously, colluding with other Byzantine processes in an attempt to manipulate the system state or violate its guarantees, deliberately delaying or accelerating the delivery of messages to selected nodes so as to disrupt

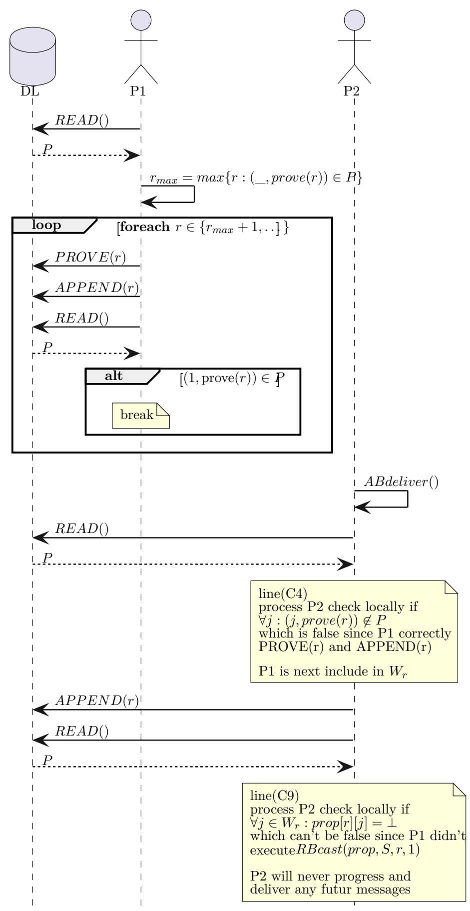

Figure 2: Example execution of the ARB algorithm with a byzantine process

the expected timing of operations, or withholding messages and responses in order to induce inconsistencies in the system state.

Byzantine processes are constrained by the following. They cannot forge valid cryptographic signatures or threshold shares without access to the corresponding private keys. They cannot violate the termination, validity, or anti-flickering properties of the DL object. They also cannot break the integrity, no-duplicates, or validity properties of the RB primitive.

Notation. Let Π be the finite set of process identifiers. Two authorization subsets are $M \subseteq \Pi$ (processes allowed to issue APPEND) and $V \subseteq \Pi$ (processes allowed to issue PROVE). Indice $i \in \Pi$ refer to processes, and p_i denotes the process with identifier i. Let $\mathcal{M}$ denote the universe of uniquely identifiable messages, with $m \in \mathcal{M}$. Let $\mathcal{R} \subseteq \mathbb{N}$ be the set of round identifiers; we write $r \in \mathcal{R}$ for a round. We use the precedence relation $\prec_k$ for the DL_k linearization: $x \prec_k y$ means that operation x appears strictly before y in the linearized history of DL_k. For any finite set $A \subseteq \mathcal{M}$, $\mathsf{ordered}(A)$ returns a deterministic total order over A (e.g., lexicographic order on $(\mathit{senderId}, \mathit{messageId})$ or on message hashes). For any round $r \in \mathcal{R}$, define $\mathsf{Winners}_r^i \triangleq \{\, j \in \Pi \mid (j, \mathsf{prove}(r)) \prec_k \mathsf{APPEND}(r) \,\}$, i.e., the set of processes whose $\mathsf{PROVE}(r)$ appears before the first $\mathsf{APPEND}(r)$ in the DL_k linearization. By extension for the set X which contains every DL we define $\mathsf{Winners}_r \triangleq \bigcup_{k \in X} \mathsf{Winners}_r^k$. We denoted by $\mathsf{PROVE}^{(j)}(r)$ or $\mathsf{APPEND}^{(j)}(r)$ the operation $\mathsf{PROVE}(r)$ or $\mathsf{APPEND}(r)$ invoked by process j, and by $\mathsf{PROVE}^{(j)}_{(k)}(r)$ or $\mathsf{APPEND}^{(j)}_{(k)}(r)$ the same operation invoked on the DL_k object.

5.2 Primitives

5.2.1 t-BFT-DL

We consider a t-Byzantine Fault Tolerant DenyList (t-$\mathsf{BFT\text{-}DL}$) with the following properties. There are 3 operations : $\mathsf{BFT\text{-}PROVE}(x), \mathsf{BFT\text{-}APPEND}(x), \mathsf{BFT\text{-}READ}(x)$ such that :

Termination. Every operation $\mathsf{BFT\text{-}APPEND}(x)$, $\mathsf{BFT\text{-}PROVE}(x)$, and $\mathsf{BFT\text{-}READ}()$ invoked by a correct process always returns.

PROVE Validity. The invocation of $op = \mathsf{BFT\text{-}PROVE}(x)$ by a correct process is valid iff there exist a set of correct process C such that $\forall c \in C$, c invoke $op_2 = \mathsf{BFT\text{-}APPEND}(x)$ with $op_2 \prec op_1$ and $|C| \leq t$

PROVE Anti-Flickering. If the invocation of a operation $op = \mathsf{BFT\text{-}PROVE}(x)$ by a correct process $p \in \Pi_V$ is invalid, then any $\mathsf{BFT\text{-}PROVE}(x)$ operation that appears after op in Seq is invalid.

READ Liveness. Let $op = \mathsf{BFT\text{-}READ}()$ invoke by a correct process such that R is the result of op. For all $(i, \mathsf{prove}(x)) \in R$ there exist a valid invocation of $\mathsf{BFT\text{-}PROVE}(x)$ by p_i.

READ Anti-Flickering. Let op_1, op_2 two $\mathsf{BFT\text{-}READ}()$ operations that returns respectively R_1, R_2. Iff $op_1 \prec op_2$ then $R_2 \subseteq R_1$. Otherwise $R_1 \subseteq R_2$.

READ Safety. Let op_1, op_2 respectively a valid $\mathsf{BFT\text{-}PROVE}(x)$ operation submited by the process p_i and a $\mathsf{BFT\text{-}READ}()$ operation submited by any correct process such that $op_1 \prec op_2$. Let R the result of op_2 then $R \ni (i, \mathsf{prove}(x))$

5.3 DL $\Rightarrow$ t-BFT-DL

Fix $3t < |M|$. Let

$$\mathcal{U} = \{\, U \subseteq M \mid |U| = |M| - t \,\}.$$

For each $U \in \mathcal{U}$, we instantiate one DenyList object DL_U whose authorization sets are

$$\Pi_M(DL_T) = S_T = U \qquad \text{and} \qquad \Pi_V(DL_T) = V.$$

$$|\mathcal{U}| = \binom{|M|}{|M| - t}.$$

Algorithm D t-BFT-DL implementation using multiple DL objects

```
function BFT-APPEND(x)
    for each U ∈ 𝒰 st i ∈ U do
        DL_U.APPEND(x)
    end for
end function

function BFT-PROVE(x)
    state ← false
    for each U ∈ 𝒰 do
        state ← state OR DL_U.PROVE(x)
    end for
    return state
end function

function BFT-READ(⊥)
    results ← ∅
    for each U ∈ 𝒰 do
        results ← results ∪ DL_U.READ()
    end for
    return results
end function
```

Lemma 20 (BFT-PROVE Validity)**.** *The invocation of op* $=$ *BFT-PROVE*(x) *by a correct process is invalid iff there exist at least* $t+1$ *distinct processes in* M *that invoked a valid BFT-APPEND*(x) *before op in* Seq*.*

Proof. Let *op* $=$ BFT-PROVE(x) be an invocation by a correct process p_i. Let $A \subseteq M$ be the set of distinct issuers that invoked BFT-APPEND(x) before *op* in Seq.

- **Case (i):** $|A| \geq t+1$**.** Fix any $U \in \mathcal{U}$. $A \cap U \neq \emptyset$. Pick $j \in A \cap U$. Since $j \in U$, the call BFT-APPEND$^{(j)}(x)$ triggers DL_U.APPEND(x), and because BFT-APPEND$^{(j)}(x) \prec op$ in Seq, this induces a valid DL_U.APPEND(x) that appears before the induced DL_U.PROVE(x) by p_i. By **PROVE Validity** of DL, the induced DL_U.PROVE(x) is invalid. As this holds for every $U \in \mathcal{U}$, there is *no* component DL_U where PROVE(x) is valid, so the field *state* at line DL9 is never becoming true, and *op* return false.

- **Case (ii):** $|A| \le t$**.** There exists $U^\star \in \mathcal{U}$ such that $A \cap U^\star = \emptyset$. For any $j \in A$, we have $j \notin U^\star$, so $\mathsf{BFT\text{-}APPEND}^{(j)}(x)$ does *not* call $DL_{U^\star}.\mathsf{APPEND}(x)$. Hence no valid $DL_{U^\star}.\mathsf{APPEND}(x)$ appears before the induced $DL_{U^\star}.\mathsf{PROVE}(x)$. Since also $i \in \Pi_V(DL_{U^\star})$, by **PROVE Validity** of DL the induced $DL_{U^\star}.\mathsf{PROVE}(x)$ is valid. Therefore, there exists a component with a valid $\mathsf{PROVE}(x)$, so *op* is valid.

Combining the cases yields the claimed characterization of invalidity. □

Lemma 21 (BFT-PROVE Anti-Flickering)**.** *If the invocation of a operation $op = \mathsf{BFT\text{-}PROVE}(x)$ by a correct process $p \in \Pi_V$ is invalid, then any $\mathsf{BFT\text{-}PROVE}(x)$ operation that appears after op in* Seq *is invalid.*

Proof. Let $op = \mathsf{BFT\text{-}PROVE}(x)$ be an invocation by a correct process p_i that is *invalid* in Seq. By BFT-PROVE Validity, this implies that there exist at least $t+1$ *distinct* processes in M that invoked a *valid* $\mathsf{BFT\text{-}APPEND}(x)$ before *op* in Seq. Let $A \subseteq M$ denote that set, with $|A| \ge t+1$.

Fix any $U \in \mathcal{U}$. We have $A \cap U \neq \emptyset$. Pick $j \in A \cap U$. Since $j \in U$, the call $\mathsf{BFT\text{-}APPEND}^{(j)}(x)$ triggers a call $DL_U.\mathsf{APPEND}(x)$. Moreover, because $\mathsf{BFT\text{-}APPEND}^{(j)}(x) \prec op$ in Seq, the induced $DL_U.\mathsf{APPEND}(x)$ appears before the induced $DL_U.\mathsf{PROVE}(x)$ of *op* in the projection Seq_U.

Hence, in Seq_U, there exists a *valid* $DL_U.\mathsf{APPEND}(x)$ that appears before the $DL_U.\mathsf{PROVE}(x)$ induced by *op*. By **PROVE Validity** the base DL object, the induced $DL_U.\mathsf{PROVE}(x)$ is therefore *invalid* in Seq_U.

Let $op' = \mathsf{BFT\text{-}PROVE}(x)$ be any invocation such that $op \prec op'$ in Seq. Fix again any $U \in \mathcal{U}$. Hence, the $DL_U.\mathsf{PROVE}(x)$ induced by op' appears after the $DL_U.\mathsf{PROVE}(x)$ induced by *op* in Seq_U. Since the induced $DL_U.\mathsf{PROVE}(x)$ of *op* is invalid, by **PROVE Anti-Flickering** of DL, *every* subsequent $DL_U.\mathsf{PROVE}(x)$ in Seq_U is invalid.

As this holds for every $U \in \mathcal{U}$, there is no component DL_U in which the induced $\mathsf{PROVE}(x)$ of op' is valid. □

Lemma 22 (BFT-READ Liveness)**.** *Let $op = \mathsf{BFT\text{-}READ}()$ invoke by a correct process such that R is the result of op. For all $(i, \mathsf{prove}(x)) \in R$ there exist a valid invocation of $\mathsf{BFT\text{-}PROVE}(x)$ by p_i.*

Proof. Let R the result of a $READ()$ operation submit by any correct process. $(i, \mathsf{prove}(x)) \in R$ implie that $\exists U^\star \in \mathcal{U}$ such that $(i, \mathsf{prove}(x)) \in R^{U^\star}$ with $R^{U^\star}$ the result of $DL_{U^\star}.\mathsf{READ}()$. By **READ Validity** $(i, \mathsf{prove}(x)) \in R^{U^\star}$ implie that there exist a valid $DL_{U^\star}.\mathsf{PROVE}^{(i)}(x)$. The for loop in the $\mathsf{BFT\text{-}PROVE}(x)$ implementation return true iff there at least one valid $DL_U.\mathsf{PROVE}^{(i)}(x)$ for any $U \in \mathcal{U}$.

Hence because there exist a $U^\star$ such that $DL_{U^\star}.\mathsf{PROVE}^{(i)}(x)$, there exist a valid $\mathsf{BFT\text{-}PROVE}^{(i)}(x)$.
$(i, \mathsf{prove}(x)) \in R \implies \exists \mathsf{BFT\text{-}PROVE}^{(i)}(x)$ □

Lemma 23 (BFT-READ Anti-Flickering)**.** *Let op_1, op_2 two $\mathsf{BFT\text{-}READ}()$ operations that returns respectively R_1, R_2. Iff $op_1 \prec op_2$ then $R_2 \subseteq R_1$. Otherwise $R_1 \subseteq R_2$.*

Proof. Let R_1, R_2 respectively the output of two $\mathsf{BFT\text{-}READ}()$ operations op_1, op_2 such that $op_1 \prec op_2$. By the implementation of BFT-READ, $R_k = \bigcup_{U \in \mathcal{U}} R_k^U$ where R_k^U is the result of $DL_U.\mathsf{READ}()$ during op_k.

Because $op_1 \prec op_2$ for any $U \in \mathcal{U}$, the $DL_U.\mathsf{READ}()$ induced by op_1 happen before the $DL_U.\mathsf{READ}()$ induced by op_2. Hence we have for all $U, R_2^U \subseteq R_1^U$. Therefore

$$\bigcup_U R_2^U \subseteq \bigcup_U R_1^U \implies R_2 \subseteq R_1$$

□

Lemma 24 (BFT-READ Safety)**.** *Let op_1, op_2 respectively a valid BFT-PROVE(x) operation submited by the process p_i and a BFT-READ$()$ operation submited by any correct process such that $op_1 \prec op_2$. Let R the result of op_2 then $R \ni (i, \mathsf{prove}(x))$*

Proof. Let $op_1 = \mathsf{BFT\text{-}PROVE}^{(i)}(x)$ be a valid operation by a correct process p_i and $op_2 = \mathsf{BFT\text{-}READ}()$ be any $\mathsf{BFT\text{-}READ}()$ operation such that $op_1 \prec op_2$ in Seq. By BFT-PROVE Validity, there exist at most t distinct processes in M that invoked a valid $\mathsf{BFT\text{-}APPEND}(x)$ before op_1 in Seq. Let $A \subseteq M$ denote that set, with $|A| \leq t$.

There exists $U^\star \in \mathcal{U}$ such that $A \cap U^\star = \emptyset$. For any $j \in A$, we have $j \notin U^\star$, so $\mathsf{BFT\text{-}APPEND}^{(j)}(x)$ does *not* call $DL_{U^\star}.\mathsf{APPEND}(x)$. Hence no valid $DL_{U^\star}.\mathsf{APPEND}(x)$ appears before the induced $DL_{U^\star}.\mathsf{PROVE}(x)$ of op_1. Since also $i \in \Pi_V(DL_{U^\star})$, by **PROVE Validity** of DL the induced $DL_{U^\star}.\mathsf{PROVE}^{(i)}(x)$ is valid.

Now, because $op_1 \prec op_2$ in Seq, the induced $DL_{U^\star}.\mathsf{PROVE}^{(i)}(x)$ appears before the induced $DL_{U^\star}.\mathsf{READ}()$ of op_2 in $\mathsf{Seq}_{U^\star}$. By **READ Safety** of DL, the result $R^{U^\star}$ of the induced $DL_{U^\star}.\mathsf{READ}()$ contains $(i, \mathsf{prove}(x))$.

Finally, by the implementation of $\mathsf{BFT\text{-}READ}()$, we have $R = \bigcup_{U \in \mathcal{U}} R^U$, so $(i, \mathsf{prove}(x)) \in R$. ☐

Theorem 25. *For any fixed value t such that $3t < |M|$, multiple DenyList Object can be used to implement a t-Byzantine Fault Tolerant DenyList Object.*

Proof. Follows directly from the previous lemmas. ☐

5.4 Algorithm

5.4.1 Variables

Each process p_i maintains the following local variables:

`last_commited` $\leftarrow 0$
`last_delivered` $\leftarrow 0$
$\mathsf{received} \leftarrow \emptyset$
$\mathsf{delivered} \leftarrow \emptyset$
$\mathsf{prop}[r][j] \leftarrow \bot, \forall r, j$
$W[r] \leftarrow \bot, \forall r$
$\mathsf{resolved}[r] \leftarrow \bot, \forall r$
$Y[j]$ ▷ Set of n BFT-DL

```
A1 function ABroadcast(m)
A2     received ← received ∪ {m}
A3     Propose()
A4 end function
```

Proposer Job

function PROPOSE($\perp$)
  $r \leftarrow$ `last_commited`
  while $S \neq \emptyset$ with $S \leftarrow \mathsf{received} \setminus (\mathsf{delivered} \cup (\bigcup_{r'<r} \bigcup_{j \in W[r']} \mathsf{prop}[r'][j]))$ **do**
    ▷ PROP PHASE
    $\mathsf{RB\text{-}cast}(i, \mathtt{PROP}, S, \mathsf{current})$
    wait until $|\{j : |\{k : (k, \mathsf{prove}(r)) \in Y[j].\mathsf{BFT\text{-}READ}()\}| \geq t+1\}| \geq n-f$
    ▷ COMMIT PHASE
    for each $j \in \Pi$ **do** $Y[j].\mathsf{BFT\text{-}APPEND}(r)$
    $\mathsf{RB\text{-}cast}(i, \mathtt{COMMIT}, r)$
    wait until $|\mathsf{resolved}[r]| \geq n-f$
    ▷ X PHASE
    $W[r] \leftarrow \{j : |\{k : (k, \mathsf{prove}(r)) \in Y[j].\mathsf{BFT\text{-}READ}()\}| \geq t+1\}$
    $r \leftarrow r+1$
  end while
  `last_commited` $\leftarrow r$
end function

---

function ADELIVER($\perp$)
  $r \leftarrow$ `last_delivered`
  if $|\mathsf{resolved}[r]| < n-f$ **then**
    return $\perp$
  end if
  $W[r] \leftarrow \{j : |\{k : (k, \mathsf{prove}(r)) \in Y[j].\mathsf{BFT\text{-}READ}()\}| \geq t+1\}$
  if $\exists j \in W[r],\ \mathsf{prop}[r][j] = \perp$ **then**
    return $\perp$
  end if
  $M \leftarrow \bigcup_{j \in W[r]} \mathsf{prop}[r][j]$
  $m \leftarrow \mathsf{ordered}(M \setminus \mathsf{delivered})[0]$ ▷ Set m as the smaller message not already delivered
  $\mathsf{delivered} \leftarrow \mathsf{delivered} \cup \{m\}$
  if $M \setminus \mathsf{delivered} = \emptyset$ **then** ▷ Check if all messages from round r have been delivered
    `last_delivered` $\leftarrow$ `last_delivered` $+ 1$
  end if
  return m
end function

```
upon Rdeliver(j, PROP, S, r) do
    received ← received ∪ {S}
    prop[r][j] ← S
    Y[j].BFT-PROVE(r)
    Propose()
end upon

upon Rdeliver(j, COMMIT, r) do
    resolved[r] ← resolved[r] ∪ {j}
end upon
```

Everything below has to be updated

Definition 5 (BFT Closed round for i)**.** Given $Seq^{(i)}$ the linearization of the BFT-DL $Y[i]$, a round $r \in \mathcal{R}$ is *closed* in Seq iff there exist at least $n - f$ distinct processes $j \in \Pi$ such that BFT-APPEND$^{(j)}(r)$ appears in Seq$^{(i)}$. Let call BFT-APPEND$(r)^\star$ the $(n-f)^{th}$ BFT-APPEND(r).

Definition 6 (BFT Closed round)**.** A round $r \in \mathcal{R}$ is *closed* iff for all process p_i, r is closed in Seq$^{(i)}$.

5.5 Proof of correctness

Lemma 26 (BFT Stable round closure)**.** *If a round r is closed, no more BFT-PROVE(r) can be valid and thus linearized. In other words, once BFT-APPEND$(r)^\star$ is linearized, no more process can make a proof on round r, and the set of valid proofs for round r is fixed. Therefore* Winners$_r$ *is fixed.*

Proof. By definition r closed means that for all process p_i, there exist at least $n-f$ distinct processes $j \in \Pi$ such that BFT-APPEND$^{(j)}(r)$ appears in Seq$^{(i)}$. By BFT-PROVE Validity, any subsequent BFT-PROVE(r) is invalid because at least $n - f$ processes already invoked a valid BFT-APPEND(r) before it. Thus no new valid BFT-PROVE(r) can be linearized after BFT-APPEND$(r)^\star$. Hence the set of valid proofs for round r is fixed, and so is Winners$_r$. □

Lemma 27 (BFT W_r as grow only set)**.** *For any correct process p_i. If p_i computes W_r at two different times t_1 and t_2 with $t_1 < t_2$, then $W_r^{t_1} \subseteq W_r^{t_2}$.*

Proof. By the implementation, W_r is computed exclusively from the results of $\{j : (j, \mathsf{prove}(r)) \in \bigcup_{k\in\Pi} Y[k].\text{BFT-READ}()\}$.

We know by BFT-READ Anti-Flickering that for any two BFT-READ() operations op_1, op_2 such that $op_1 \prec op_2$, the result of op_2 is included in the result of op_1. Therefore, if p_i computes W_r at two different times t_1 and t_2 with $t_1 < t_2$, then $W_r^{t_1} \subseteq W_r^{t_2}$. □

Lemma 28 (BFT well defined winners)**.** *For any closed round r, if a correct process p_i compute W_r, then $W_r =$ Winners$_r$ with $|W_r| \geq n - f$.*

Proof. By Lemma 24, any correct process p_i computing W_r after round r is closed includes all valid BFT-PROVE(r) in its computation of W_r. Therefore $W_r =$ Winners$_r$.

By Definition 6, at least $n - f$ distinct processes invoked a valid BFT-APPEND(r) before BFT-APPEND$(r)^\star$. By the implementation in algorithm D, if a process correct j invoked a valid BFT-APPEND(r), thats means that he observed at least $n - f$ valid BFT-PROVE(r) submitted by distinct processes. By Lemma 27, once p_j observed $n - f$ valid BFT-PROVE(r), any correct process computing W_r will eventually observe at least these $n-f$ valid $\mathsf{BFT\text{-}PROVE}(r)$. By Lemma 26, no more valid $\mathsf{BFT\text{-}PROVE}(r)$ can be linearized after round r is closed, so any correct process computing the same fixed set W_r of at least $n-f$ distinct processes. ☐

Lemma 29 (BFT Non-empty winners proposal)**.** *For every process p_i such as $i \in W_r$, eventually $\mathsf{prop}[r][i] \neq \bot$.*

Proof. By the implementation, if $i \in W_r$, then $(i, \mathsf{prove}(r))$ is included in the result of at least one $\mathsf{BFT\text{-}READ}()$ operation. Hence there exist a valid $\mathsf{BFT\text{-}PROVE}(r)$ operation. By Lemma 20, this implies that there exist at least $f+1$ valid $\mathsf{PROVE}(r)$ operation invoked by processes. At least one of these processes is correct, say p_j. By the implementation, p_j invoked $\mathsf{BFT\text{-}PROVE}(r)$ after receiving a $Rdeliver(j, \texttt{PROP}, S, r)$ message from p_i. Therefore, by the reliable broadcast properties, the message will eventually be delivered to every correct process, hence eventually for any correct process $\mathsf{prop}[r][i] \neq \bot$. ☐

Definition 7 (BFT Message invariant)**.** For any closed round r, for any correct process p_i, such that $\nexists j \in W_r : \mathsf{prop}[r][j] = \bot$, twe define the set

$$\mathsf{Messages}_r = \bigcup_{j \in \mathsf{Winners}_r} \mathsf{prop}[r][j]$$

as the unique set of messages proposed during round r.

Lemma 30 (BFT Proposal convergence)**.** *For any closed round r, for any correct process p_i, that define M_r at line B10, we have $M_r = \mathsf{Messages}_r$.*

Proof. By Lemma 28, any correct process p_i computing W_r after round r is closed has $W_r = \mathsf{Winners}_r$. By Lemma 29, for any correct process p_i, such as $i \in W_r$, eventually $\mathsf{prop}[r][i] \neq \bot$.

Therefore, eventually for any correct process p_i, at line B10 we have

$$M_r = \bigcup_{j \in W_r} \mathsf{prop}[r][j] = \bigcup_{j \in \mathsf{Winners}_r} \mathsf{prop}[r][j] = \mathsf{Messages}_r$$

☐

Lemma 31 (BFT Inclusion)**.** *If a correct process p_i ABroadcasts a message m, then eventually any correct process p_j ADelivers m.*

Proof. Let m be a message ABroadcast by a correct process p_i and eventually exit the `ABroadcast` function at line A10.

By the implementation, if p_i exits the `ABroadcast` function at line A10, then there exists a round r' such that $m \in \mathsf{prop}[r'][j]$ for some $j \in W_{r'}$.

Since p_i is correct, seeing that $m \in \mathsf{prop}[r'][j]$ for some $j \in W_{r'}$ implies that p_i received a $Rdeliver(j, \texttt{PROP}, S, r')$ message from p_j such that $m \in S$. And because p_j is in $W_{r'}$, at least $n-f$ correct processes invoked a valid $Y[j].\mathsf{BFT\text{-}PROVE}(r')$ before the round r' were closed. By the reliable broadcast properties, the $Rdeliver(j, \texttt{PROP}, S, r')$ message will eventually be delivered to every correct process, hence eventually for any correct process $m \in \mathsf{prop}[r'][j]$ with $j \in W_{r'}$. Hence m will eventually be included in the set $\mathsf{Messages}_{r'}$ defined in Definition 7 and thus eventually be ADelivered by any correct process. ☐

Theorem 32. *The algorithm implements a BFT Atomic Reliable Broadcast.*

6 Implementation of BFT-DenyList and Threshold Cryptography

6.1 DenyList

BFT-DenyList In our algorithm we use multiple DenyList as follows:

- Let $\mathcal{DL} = \{DL_1, \ldots, DL_k\}$ be the set of DenyList used by the algorithm.
- We set $k = \binom{n}{f}$.
- For each $i \in \{1, \ldots, k\}$, let M_i be the set of moderators associated with DL_i according to the DenyList definition, so that $|M_i| = n - f$.
- Let $\mathcal{M} = \{M_1, \ldots, M_k\}$. We require that the M_i are pairwise distinct:

$$\forall i, j \in \{1, \ldots, k\},\ i \neq j \implies M_i \neq M_j.$$

Lemma 33. *$\exists M_i \in M : \forall p \in M_i$ p is correct.*

Proof. Let consider the set F of faulty processes, with $|F| = f$. We can construct the set $M_i = \Pi \setminus F$ such that $|M_i| = n - |F| = n - f$. By construction, $\forall p \in M_i$ p is correct. □

Lemma 34. *$\forall M_i \in M, \exists p \in M_i$ such that p is correct.*

Proof. $\forall i \in \{1, \ldots, k\}, |M_i| = n - f$ with $n \geq 2f + 1$. We can say that $|M_i| \geq 2f + 1 - f = f + 1 > f$ □

Each process can invoke the following functions :

- $\mathsf{READ}' : () \to \mathcal{L}(\mathbb{R} \times \mathsf{prove}(\mathbb{R}))$
- $\mathsf{APPEND}' : \mathbb{R} \to ()$
- $\mathsf{PROVE}' : \mathbb{R} \to \{0, 1\}$

Such that :

Algorithm E $\mathsf{READ}'() \to \mathcal{L}(\mathbb{R} \times \mathsf{prove}(\mathbb{R}))$

```
function READ'
    j ← the process invoking READ'()
    res ← ∅
    for all i ∈ {1, ..., k} do
        res ← res ∪ DL_i.READ()
    end for
    return res
end function
```

Algorithm F $\mathsf{APPEND}'(\sigma) \to ()$

```
function APPEND'(σ)
    j ← the process invoking APPEND'(σ)
    for all M_i ∈ {M_k ∈ M : j ∈ M_k} do
        DL_i.APPEND(σ)
    end for
end function
```

Algorithm G $\mathsf{PROVE}'(\sigma) \to \{0, 1\}$

function PROVE'(σ)
    $j \leftarrow$ the process invoking $\mathsf{PROVE}'(\sigma)$
    $flag \leftarrow false$
    for all $i \in \{1, \dots, k\}$ **do**
        $flag \leftarrow flag$ OR $DL_i.\mathsf{PROVE}(\sigma)$
    end for
    return $flag$
end function

6.2 Threshold Cryptography

We are using the Boneh-Lynn-Shacham scheme as cryptography primitive to our threshold signature scheme. With :

- $G : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$
- $S : \mathbb{R} \times \mathcal{R} \to \mathbb{R}$
- $V : \mathbb{R} \times \mathcal{R} \times \mathbb{R} \to \{0, 1\}$

Such that :

- $G(x) \to (pk, sk)$: where x is a random value such that $\nexists x_1, x_2 : x_1 \neq x_2, G(x_1) = G(x_2)$
- $S(sk, m) \to \sigma_m$
- $V(pk, m_1, \sigma_{m_2}) \to k$: with $k = 1$ iff $m_1 == m_2$ and $\exists x \in \mathbb{R}$ such that $G(x) \to (pk, sk)$; otherwise $k = 0$

threshold Scheme In our algorithm we are only using the following functions :

- $G' : \mathbb{R} \times \mathbb{N} \times \mathbb{N} \to \mathbb{R} \times (\mathbb{R} \times \mathbb{R})^n$: with $n \triangleq |\Pi|$
- $S' : \mathbb{R} \times \mathcal{R} \to \mathbb{R}$
- $C' : \mathbb{R}^n \times \mathcal{R} \times \mathbb{R} \times \mathbb{R}^t \to \{\mathbb{R}, \perp\}$: with $t \leq n$
- $V' : \mathbb{R} \times \mathcal{R} \times \mathbb{R} \to \{0, 1\}$

Such that :

- $G'(x, n, t) \to (pk, pk_1, sk_1, \dots, pk_n, sk_n)$: let define $pkc = pk_1, \dots, pk_n$
- $S'(sk_i, m) \to \sigma_m^i$
- $C'(pkc, m_1, J, \{\sigma_{m_2}^j\}_{j \in J}) \to \sigma$: with $J \subseteq \Pi$; and $\sigma = \sigma_{m_1}$ iff $|J| \geq t, \forall j \in J : V(pk_j, m_1, \sigma_{m_2}^j) == 1$; otherwise $\sigma = \perp$.
- $V'(pk, m_1, \sigma_{m_2}) \to V(pk, m_1, \sigma_{m_2})$

References

[1] Fred B. Schneider. Implementing fault-tolerant services using the state machine approach: a tutorial. *ACM Computing Surveys*, 22(4):299–319, 1990.