```
──────────────────────── MODULE IdemProxy ────────────────────────

 Expectations :
 - Every request must be hit the server exactly once
 - For each try of a request, the response must be the same
 - 2 requests must be processable in parallel

 EXTENDS Integers, FiniteSets, Sequences

 CONSTANTS
     _ReqIDs,    the request IDs sent by the user (an Id is the idempotent key)
     _MaxTries   how many times a request is retried

 ASSUME _MaxTries < 10

 VARIABLES
     requests   the state of all requests and their corresponding tries

 vars ≜ ⟨requests⟩

  tryKeys is a simple helper providing the set of try keys
 tryKeys ≜ 1 . . _MaxTries

 Initial State
 Init ≜
 requests is a struct with _ReqIDs as keys associated with structs with tryKeys as keys associatied
 with the given try current status
     ∧ requests = [req ∈ _ReqIDs ↦ [st ∈ tryKeys ↦ "pending"]]


 TypeInvariants ≜
   ∧ TRUE  todo


 Actions
 HitProxy(r, i) ≜
     ∧ requests[r][i]    = "pending"
     ∧ Cardinality({x ∈ DOMAIN requests[r] :
                 ∨ requests[r][x] = "submitted"
                 ∨ requests[r][x] = "processed"}
           ) = 0  add a blocking thread
     ∧ requests′ = [requests EXCEPT ![r][i] = "submitted"]


 HitServer(r, i) ≜
     ∧ requests[r][i] = "submitted"
     ∧ requests′ = [requests EXCEPT ![r][i] = "processed"]
```

Spec

```
$Next \triangleq$
  $\lor \exists\, r \in \_ReqIDs,\ i \in tryKeys :$
     $\lor HitProxy(r,\ i)$
     $\lor HitServer(r,\ i)$

$Fairness \triangleq \forall\, r \in \_ReqIDs,\ i \in tryKeys :$
                        $\land \text{SF}_{vars}(HitServer(r,\ i))$
                        $\land \text{SF}_{vars}(HitProxy(r,\ i))$

$Spec \triangleq$
  $\land Init$
  $\land \Box[Next]_{vars}$
  $\land Fairness$

$RequestIsProcessedOnlyOnce \triangleq$
     $\Box(\forall\, req \in \text{DOMAIN } requests :$
        $Cardinality(\{x \in \text{DOMAIN } requests[req] : requests[req][x] = \text{“processed”}\}) < 2)$

$AttemptsAreProcessedConcurrently \triangleq$
     $\Diamond(\forall\, req \in \text{DOMAIN } requests :$
        $Cardinality(\{x \in \text{DOMAIN } requests[req] : requests[req][x] = \text{“submitted”}\}) > 1)$

THEOREM $Spec \Rightarrow RequestIsProcessedOnlyOnce$
```