

- Read local message  $m$  (from  $Z$ ). Pick a random nonce  $n \in \{0, 1\}^\kappa$  and issue query  $h = H(h_{-1}, \eta, m)$  where  $h_{-1}$  is the 4'th element in the last block in *chain*. If  $h < D_p$ , then  $\Pi$  adds the *newly mined* block  $(h_{-1}, \eta, b, h)$  to *chain* and broadcasts the updated *chain*.