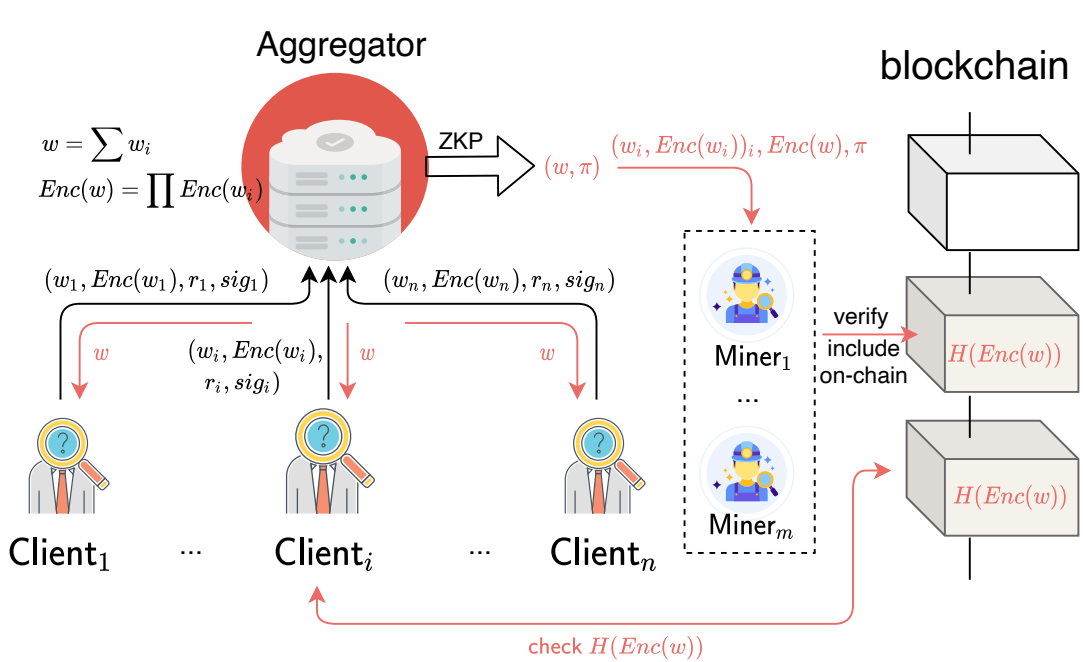
Aggregator
blockchain
$w = \sum w_i$
$Enc(w) = \prod Enc(w_i)$
ZKP
(w, π)
$(w_i, Enc(w_i))_i, Enc(w), \pi$
$(w_1, Enc(w_1), r_1, sig_1)$
$(w_n, Enc(w_n), r_n, sig_n)$
w
$(w_i, Enc(w_i), r_i, sig_i)$
w
w
Miner$_1$
...
Miner$_m$
verify
include
on-chain
$H(Enc(w))$
$H(Enc(w))$
Client$_1$
...
Client$_i$
...
Client$_n$
check $H(Enc(w))$