$$\boxed{\text{hash}_0} \rightarrow \boxed{\text{hash}_1} \rightarrow \boxed{\text{hash}_2} \rightarrow \bullet \bullet \bullet \rightarrow \boxed{\text{hash}_n}$$

off-chain —————— efficient   secure

Does the solution
require a change in
blockchain protocol?

How likely is it that
Is the solution affected
attackers will fool the
by chain length?
system?