Cryptography Blockchain

Lab 3 - SHA-512

Lab Report

CARVAJAL Mateo
CHAHINE Maroun
DOS ANJOS GUIMARAES Bernardo

5IF | OT4
December 2025

Analysis of first *p* bits in a hash value *h.*

Our results can be found in the CSV file. The source code for each exercise of our implementation of SHA-512 are also available in the py files and named respectively.

The time required to find a hash value ***h*** with ***p*** leading zero bits was evaluated for values of ***p*** = 1, 2 , 3, 4,…,10

A random value was assigned to ***id*** (in bytes), and the value ***x*** was incremented starting from 0. The search space for ***x*** was limited to a maximum of $\mathbf{2^{64}}$ possible values, corresponding to a 64-bit nonce space.

To prevent excessively long executions, a maximum execution time of 600 seconds (10 minutes) was imposed for each value of ***p***

The results obtained are shown in Figure X.

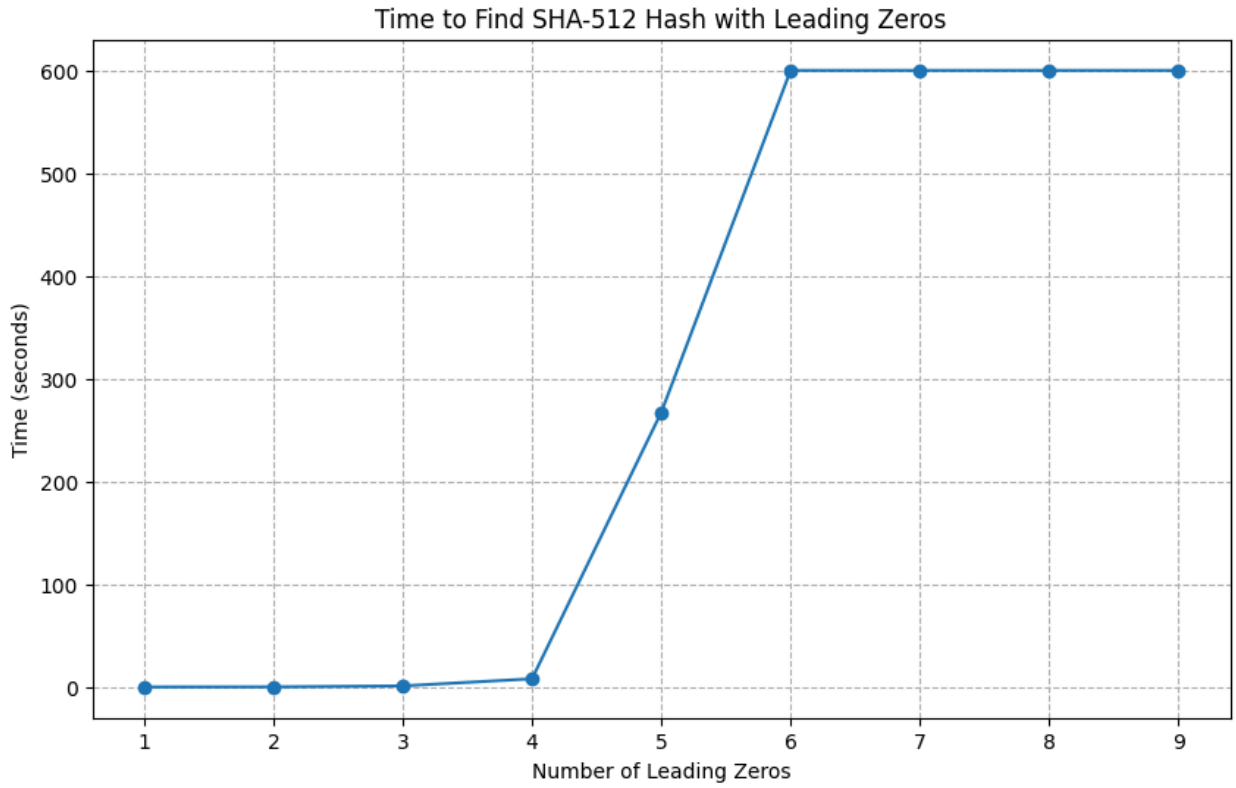

Figure X: Time to find a SHA-512 hash with p leading zeros

As shown in Figure X, the execution time remains very small for low values of ***p*** (from 1 to 4). In this range, valid values of ***x*** are found almost immediately, which is consistent with the relatively high probability of success.

A significant increase in execution time is observed starting from $\boldsymbol{p} = 5$ This sharp rise reflects the exponential nature of the search problem: the probability of finding a hash with $\boldsymbol{p}$ leading zero bits is equal to 2^{-p^2}, which implies that the expected number of trials doubles each time ppp increases by one.

For values of $\boldsymbol{p} \geq 6$, the execution time reaches the imposed timeout limit of 600 seconds, and no solution is found within the allowed time. The plateau observed in the graph therefore does not indicate a stabilization of the problem's difficulty, but rather the experimental limit set to avoid excessive computation.