

SHA-256 Hash Space: Incomprehensibly Large

2^{256}

= 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,936

Atoms in Universe

$\sim 10^{80}$

Hash space is 10^{77} times larger!

Grains of Sand on Earth

$\sim 10^{23}$

Hash space is 10^{54} times larger!

Seconds Since Big Bang

$\sim 10^{17}$

Hash space is 10^{60} times larger!

Probability of collision: Winning the lottery every day for a billion years

This massive space makes brute-force attacks computationally infeasible