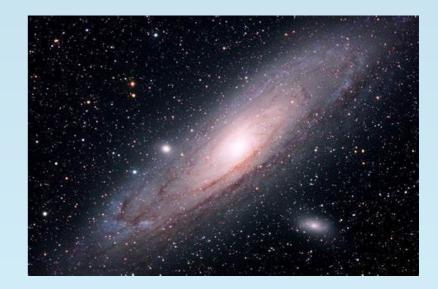
## Hash Space is Effectively Infinite

## Why is it so hard to guess?

If hash bits are random,
the chance that a forged document
has the same 64-Byte (512-bit) hash
is 1 in 2<sup>512</sup>, or about 1 in 10<sup>155</sup>.

One-way hash functions ° are thus considered unbreakable ° ... for now.



only 10<sup>80</sup> particles in the observable universe