BLOCKCHAIN TUTORIAL 3

Hash

BLOCKCHAIN TUTORIAL 3

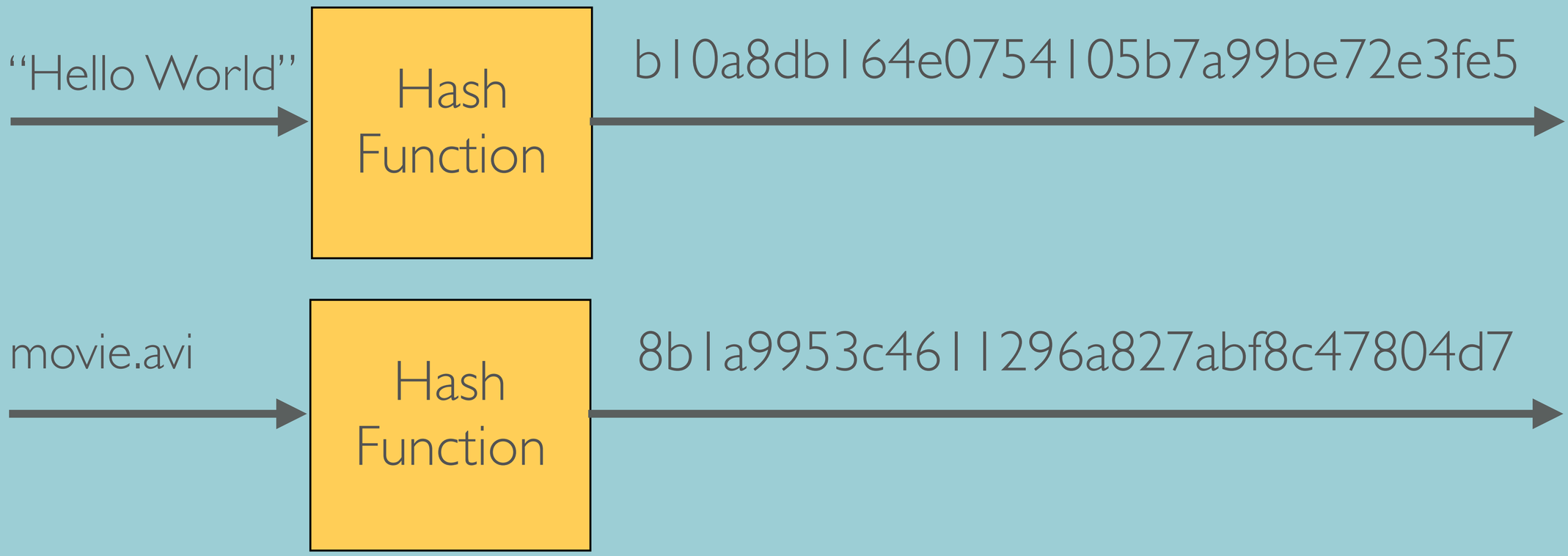
Hash

HASH

- A hash function converts data of any size into a string of a fixed size
- A small change in the data will result in a complete different hash
- When to different inputs produces the same hash, it is called a hash collision
- A hash function is considered "collision resistant" when it is very hard to find two inputs that hash to the same output
- There are many different hash functions

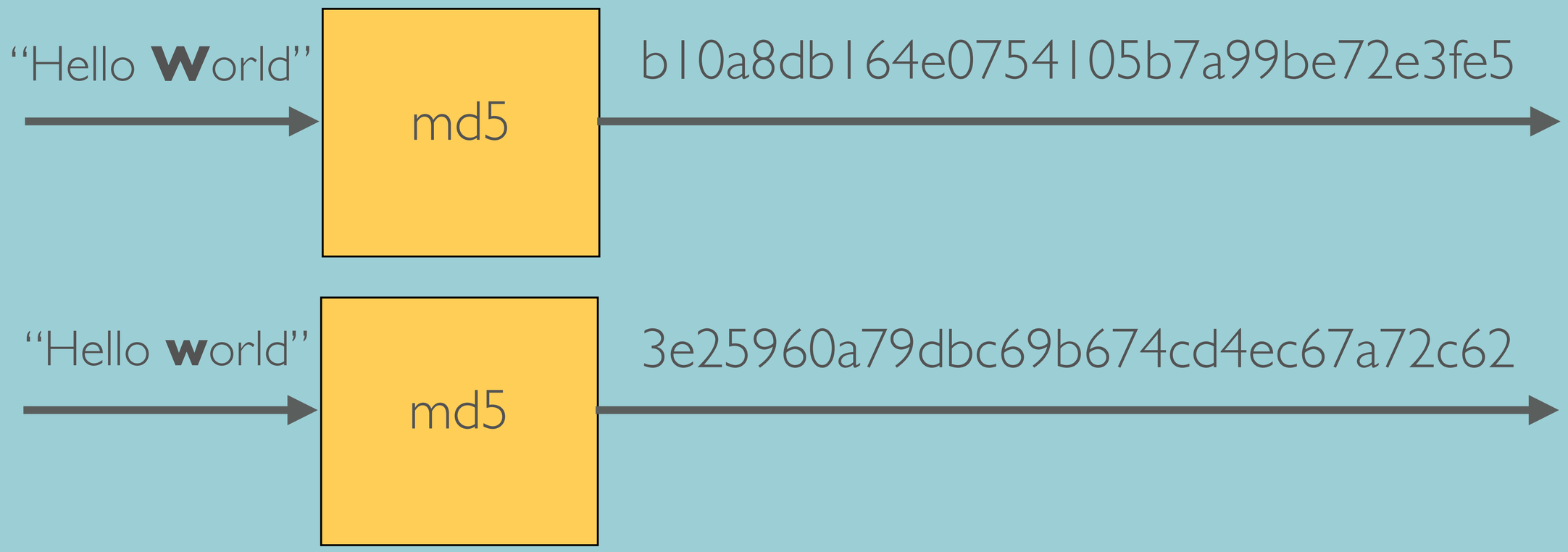
HASH

A hash function converts data of any size into a string of a fixed size



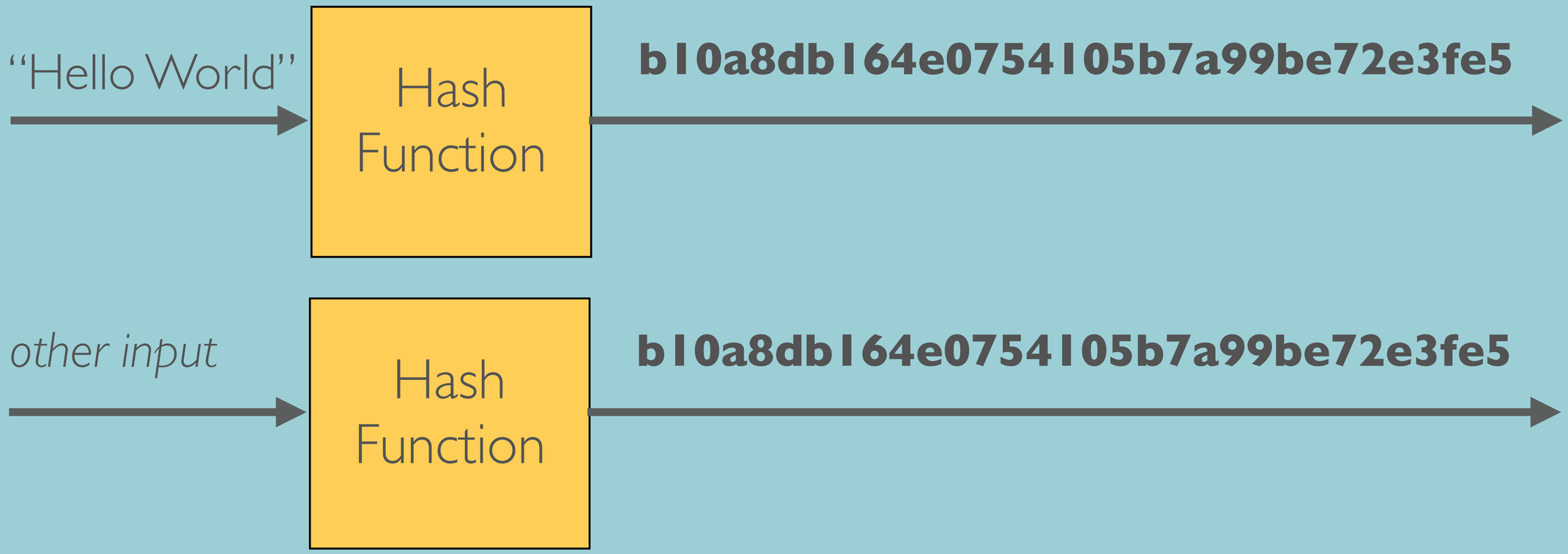
HASH

A small change in the data will result in a complete different hash



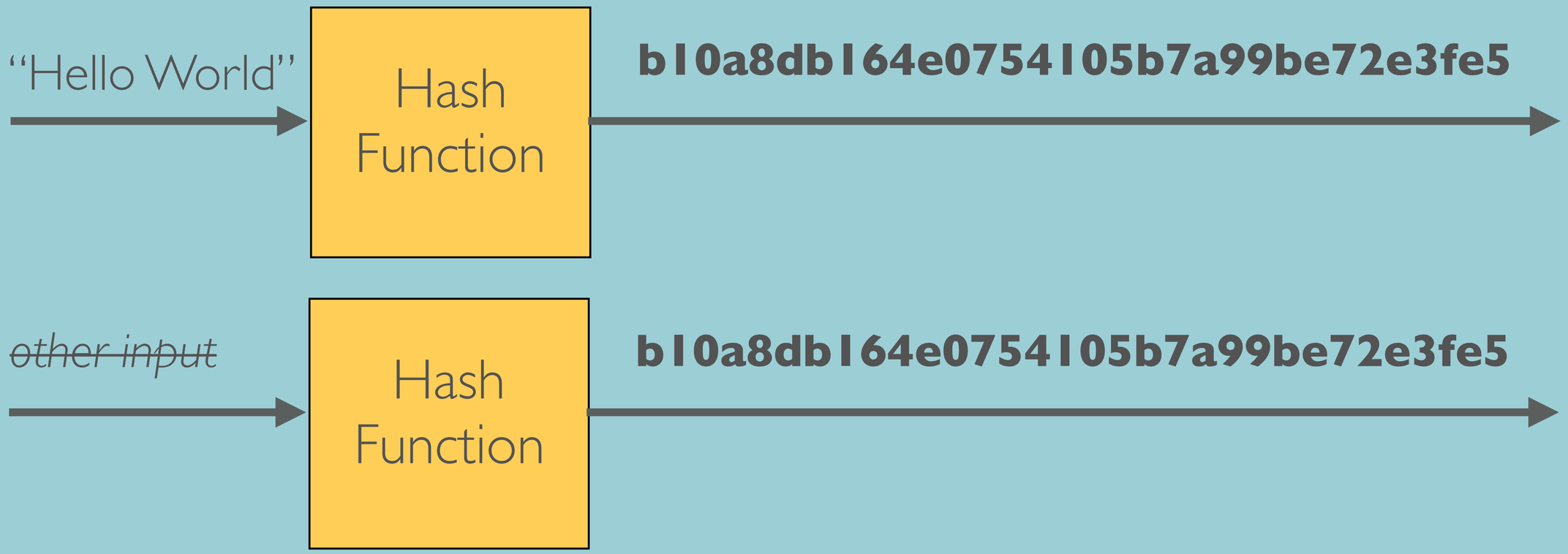
HASH

When to different inputs produces the same hash, it is called a hash collision



HASH

A hash function is considered "collision resistant" when it is very hard to find two inputs that hash to the same output



HASH FUNCTION

There are many different hash functions. Here are just a few:

Hash function	Hash length	Secure
md5	128 bits (32 symbols)	No *
ripemd160	160 bits (40 symbols)	Yes
sha1	160 bits (40 symbols)	No *
sha256	256 bits (64 symbols)	Yes
keccak-256	256 bits (64 symbols)	Yes

md = message digest

ripemd = RACE integrity primitives evaluation message digest

sha = secure hash algorithm

* not collision resistant