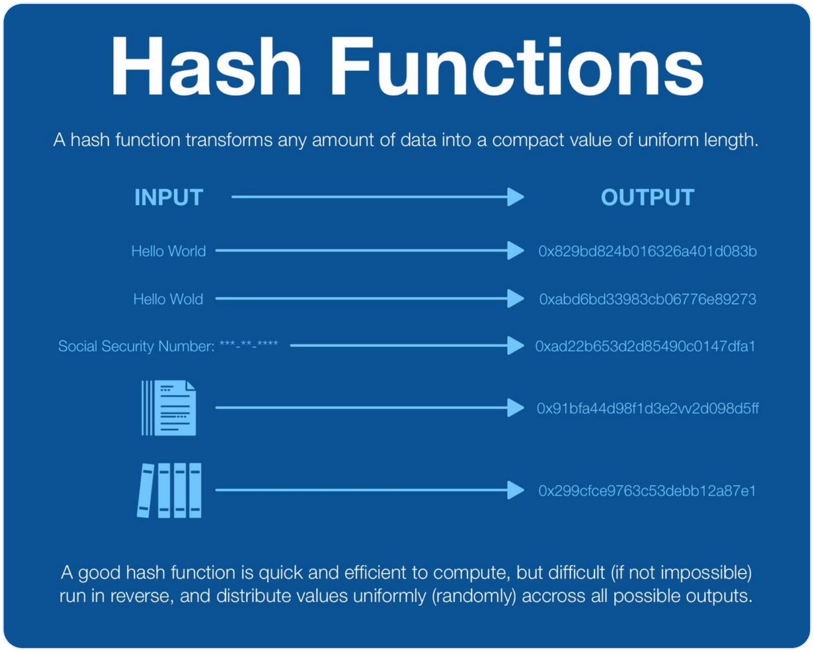
Haym Salomon @SalomonCrypto

Sep 7 • 8 tweets • SalomonCrypto/status/1567541750151151616

(1/7) Computer Science 101: Hash Functions

What is a hash function? What are the characteristics of a good hash function? Where do hash functions appear and why do I hear about them all the time?

If you want to understand the fundamental tool of crypto, this guide is for you!



Hash Functions

A hash function transforms any amount of data into a compact value of uniform length.

INPUT → OUTPUT

Hello World → 0x829bd824b016326a401d083b

Hello Wold → 0xabd6bd33983cb06776e89273

Social Security Number: ***-**-**** → 0xad22b653d2d85490c0147dfa1

→ 0x91bfa44d98f1d3e2vv2d098d5ff

→ 0x299cfce9763c53debb12a87e1

A good hash function is quick and efficient to compute, but difficult (if not impossible) run in reverse, and distribute values uniformly (randomly) accross all possible outputs.

(2/7) The purpose of a hash function is to transform any amount of data into a compact, uniform value. The input can be of arbitrary length but the output is always the same length.

The length is decided by the hash function; it can be as small or large as desired.

(3/7) Hash functions have many different uses, but all uses rely on the same fundamental properties:

- quick and efficient to compute
- outputs should be randomly distributed between all possible outputs
- difficult (if not impossible) to reverse engineer an input from an output

(4/7) If your hashing function has an output with 3 characters and you feed it 1MM pieces of data, much of it will result in the same output.

However, if the output is long enough, a good hash function will have no collisions (two inputs resulting in the same output).

(5/7) With a strong hashing function, we have the ability to take any data and compress it into a verifiable signature.

If the data is public, then anyone can recreate the signature and verify that the data matches its label.

(6/7) If the data is private, it can form the basis of identity.

Any private information fed into a (good) hash function will instantly become lost but form the basis of a unique, un-replicable signature.

(7/7) From here, we can go further: signatures created by two private identities can create a 3rd shared secret - the basis of encryption.

Encryption, cryptography, cryptocurrency When it comes down to it... hash functions are the foundation of crypto!

https://www.tutorialspoint.com/cryptography/cryptography_hash_functions.htm

Like what you read? Help me spread the word by retweeting the thread (linked below).

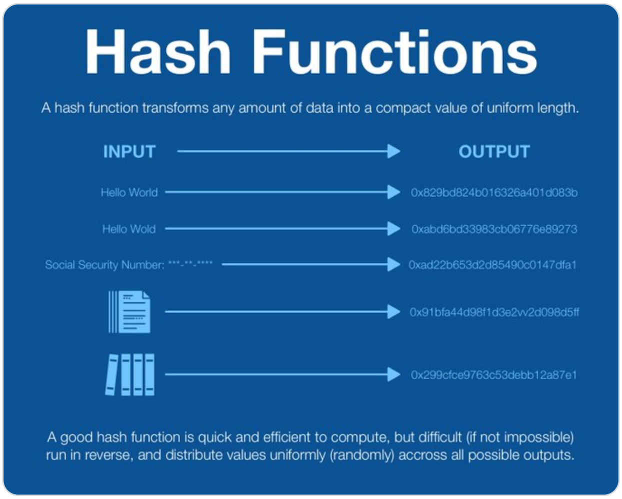
Follow me for more explainers and as much alpha as I can possibly serve.

Haym Salomon
@SalomonCrypto · **Follow**

(1/7) Computer Science 101: Hash Functions

What is a hash function? What are the characteristics of a good hash function? Where do hash functions appear and why do I hear about them all the time?

If you want to understand the fundamental tool of crypto, this guide is for you!



Hash Functions

A hash function transforms any amount of data into a compact value of uniform length.

INPUT
OUTPUT
Hello World
0x829bd824b016326a401d083b
Hello Wold
0xabd6bd33983cb06776e89273
Social Security Number: ***-**-****
0xad22b653d2d85490c0147dfa1
0x91bfa44d98f1d3e2vv2d098d5ff
0x299cfce9763c53debb12a87e1

A good hash function is quick and efficient to compute, but difficult (if not impossible) run in reverse, and distribute values uniformly (randomly) accross all possible outputs.

3:54 PM · Sep 7, 2022

Read the full conversation on Twitter

100 Reply Copy link

Read 1 reply

• • •