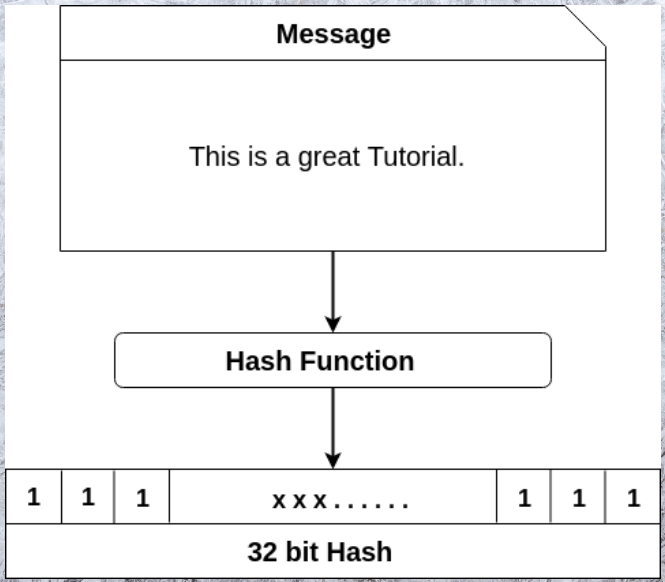
Blockchain Snippets

BLOCKCHAIN HASH FUNCTION

- A HASH FUNCTION TAKES AN INPUT STRING (NUMBERS, ALPHABETS, MEDIA FILES) OF ANY LENGTH AND TRANSFORMS IT INTO A FIXED LENGTH.
- THE FIXED BIT LENGTH CAN VARY (LIKE 32-BIT OR 64-BIT OR 128-BIT OR 256-BIT) DEPENDING ON THE HASH FUNCTION WHICH IS BEING USED.
- THE FIXED-LENGTH OUTPUT IS CALLED A HASH. THIS HASH IS ALSO THE CRYPTOGRAPHIC BYPRODUCT OF A HASH ALGORITHM.
- WE CAN UNDERSTAND IT FROM THE FOLLOWING DIAGRAM


Message
This is a great Tutorial.
Hash Function
1
1
1
x x x . . . . . .
1
1
1
32 bit Hash

- THE HASH ALGORITHM HAS CERTAIN UNIQUE PROPERTIES:IT PRODUCES A UNIQUE OUTPUT (OR HASH).
- IT IS A ONE-WAY FUNCTION.
- IN THE CONTEXT OF CRYPTOCURRENCIES LIKE BITCOIN, THE BLOCKCHAIN USES THIS CRYPTOGRAPHIC HASH FUNCTION'S PROPERTIES IN ITS CONSENSUS MECHANISM.
- A CRYPTOGRAPHIC HASH IS A DIGEST OR DIGITAL FINGERPRINTS OF A CERTAIN AMOUNT OF DATA.

SHA-256

- A BITCOIN'S BLOCKCHAIN USES SHA-256 (SECURE HASH ALGORITHM) HASHING ALGORITHM. IN 2001, SHA-256 HASHING ALGORITHM WAS DEVELOPED BY THE NATIONAL SECURITY AGENCY (NSA) IN THE USA.

SHA256 HASH

SHA256 Hash

Data:

Hash: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

- If we type any character in the data section, we will observe its corresponding cryptographic hash in the hash section.
- For example, We have type in the data section: This is a great tutorial.
- It will generate the corresponding Hash:

759831720aa978c890b11f62ae49d2417f600f26aaa51b3291a8d21a4216582a