SHA256 Hash

* What is the SHA256 Hashing Algorithm? is t

he SHA

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of 512 = 16 × 32 bits, each block

requiring 64 rounds.

SHA256 stands for Secure Hash Algorithm 256-bit and it’s used for cryptographic security.

Cryptographic hash algorithms produce irreversible and unique hashes. The larger the number of possible hashes, the smaller the chance that two values will create the same hash.

A hash is as a mathematical computer process that takes information and turns it into letters and numbers of a certain length. Hashing is used to make storing and finding information quicker because hashes are usually shorter and easier to find. Hashes also make information unreadable and so the original data can become confidential.

For example, “I like bitcoin” can be hashed and will equal: ad3e58f21b94f32dcadca6b71df4c31a18179f38011551a17a80d0ff065d22c5

If I were to capitalize the “b” in bitcoin, so it says, “I like Bitcoin” the hash will be completely different: d988ca30eaa88c0410ad6e48a5297c0d505dcee572f9884f1a6fa2cbc8dedc86

The number of possible combinations of letters and numbers produced by SHA 256 exceeds the number grains of sand on Earth! That makes guessing the data hidden within the hash virtually impossible. Hashes cannot be reversed, so the process is typically used for computer security.

* **Some 256 Hash codes for example**

ad3e58f21b94f32dcadca6b71df4c31a18179f38011551a17a80d0ff065d22c5

d988ca30eaa88c0410ad6e48a5297c0d505dcee572f9884f1a6fa2cbc8dedc86

**Basic operations**

• Boolean operations AND, XOR and OR, denoted by ∧, ⊕ and ∨, respectively.

• Bitwise complement, denoted by ¯.

• Integer addition modulo 232, denoted by A + B.

Each of them operates on 32-bit words. For the last operation, binary words are interpreted as integers written in base 2.

• RotR(A, n) denotes the circular right shift of n bits of the binary word A.

• ShR(A, n) denotes the right shift of n bits of the binary word A.

• AkB denotes the concatenation of the binary words A and B.

Reference-some pdf over internet