Hash Functions and Proof of Stake

Hieu Nguyen

Fulbright University Vietnam

May 5, 2023

Hash Functions

- Hash functions are used in different areas not just in cryptocurrency
- Even in cryptocurrency, hash functions are used for different purposes

Hash function

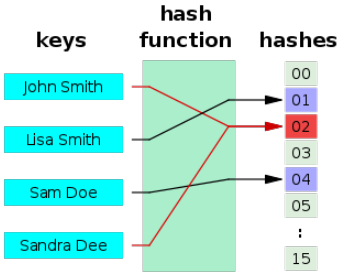
Definition

A **hash function** is any *function* that can be used to map *data* of arbitrary size to fixed-size values.

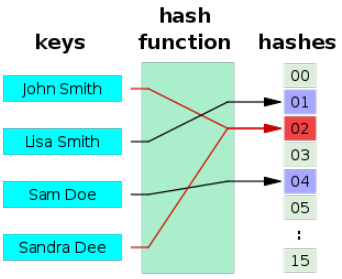
Hash function

Definition

A **hash function** is any *function* that can be used to map *data* of arbitrary size to fixed-size values.



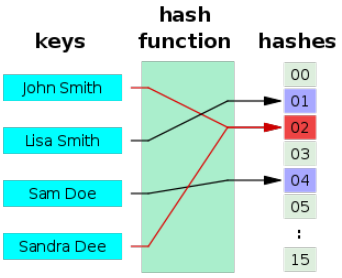
Hash function



- Input: a string, a SMS, a picture, a mp3 file, an application, etc

The hash values are usually used to index a fixed-size table called a hash table.

Hash function



- Input: a string, a SMS, a picture, a mp3 file, an application, etc
- Output: output values are called hash values, hash codes, digests or simply hashes.

The hash values are usually used to index a fixed-size table called a hash table.

Hash Table

- Hash Table

Hash Functions and Some Practical Usages

- Hash Functions

Some Popular Hash Functions

- MD5

Some Popular Hash Functions

- MD5
- SHA-2 (Secure Hash Algorithm 2) family: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256

Some Popular Hash Functions

- MD5
- SHA-2 (Secure Hash Algorithm 2) family: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256
- Keccak256 (a variant of SHA3-256)

Cryptographic Hash Functions

- Cryptographic Hash Functions

How Secure is SHA256?

- How Secure is SHA256?

Hash Functions in a Blockchain

- How does a blockchain work

Hash Functions in Proof of Work

- Hash Functions in Proof of Work

Proof of Stake

- What is Proof of Stake