

## Hashing

Hashing is a cryptographic technique that applies a mathematical function (hash algorithm) to convert data of an arbitrary size into a new digital string of a predefined and fixed length – a hash (see the example below and Prpic, 2017).

Example of hashing

| INPUT   | HASH   |
|---------|--|
| Hi      | 639EFCDD08ABB273B1619E82E78C29A7DF02C1051B1820E99FC395DCAA3326B8 |
| Welcome | 53A53FC9E2A03F9B6E66D84BA701574CD9CF5F01FB498C41731881BCDC68A7C8 |

Source: <https://blockgeeks.com/guides/what-is-hashing/>

Hashing has several properties that make it an interesting tool to ensure data integrity and prevent forgery:

- A set of data (input) will always give the same hash (output). This is important when it comes to verifying the integrity of data. If a piece of information produces different hashes for the sender and the receiver, this means that it has been tampered with during transit.
- Hashing is often referred to as “one-way encryption” because it is extremely difficult to determine the original input from its hash value. The probability of “guessing” it would require a daunting amount of computational power.
- Hash functions are very efficient: computing an output from an input is very rapid.
- Hash functions are “puzzle-friendly”: if an output is obtained by combining two sets of input (concatenated), it is nearly impossible to identify the value of one of them if the second is already known.
- Hash functions are “collision-resistant”: the likelihood that two different inputs would randomly give the same outputs is extremely limited.

## Hyperledger Fabric

Hyperledger is an open-source collaborative effort created to act as a foundation for developing blockchain-based products, solutions and applications for use by private enterprises. It is a global collaboration, hosted by The Linux Foundation, including leaders in finance, banking, IoT, supply chains, manufacturing and technology.