

Hash it Out!

Descriere

AcadNet 2021

Author: Alexandru Razvan Caciulescu

Welcome to the "Hash it out" challenge!

During your journey to implementing your new crypto coin you stumble upon the importance of hashing! In order to provide the integrity of your new blockchain you must implement a (decent enough) hashing function that binds together your blocks.

What is a hashing function? It's a function that can takes input of any sizes and return a (relatively) fixed-size value output. It has a few key properties:

- determinism: for a specific input it will *always* return the same output.
- uniformity: the output values should be as spread out as evenly as possible.
- few collisions. A collision happens when the hash of two different input values is the same.

Your task is to implement a function with the signature `unsigned long string_hash(unsigned char *string)`.

Download resources [here](#).

Background info

For this year we prepared a 3+1 challenge approach (3 themed challenges + 1 old friend). With all the recent hype and market fluctuation, we think it's the perfect time you understand some of the basics behind cryptocurrencies and how you could implement (a simplified) blockchain from scratch. HODL on before you jump into the challenges, a quick dive into blockchain theory might give you a better understanding of how to tackle them.

What is a blockchain? In short it's a list of records, called blocks, that are tied together using cryptography. Each block includes the cryptographic hash of the previous one, reinforcing the link with the ones before and after it. Each new hash is calculated by taking into account the data of the current block and the hash of the previous one. This means that if someone wanted to retroactively modify a transaction in a block they would have to change ALL of the subsequent blocks. Why is this almost impossible to do? Because the blockchain is growing at an insane speed due to the fact that any number of different users contribute and add new blocks every second, thus making it impossible for a malicious actor to catch up.

That's the simplified version, at least!

TL;DR that's how Bitcoin came into existence in 2008 and reached the insane price of ~\$65.000 at its peak.

Note

- the file you will submit will contain *only* the `string_hash` function
- the submitted file can have a maximum of 15 lines
- the submitted file can have a maximum of 50 chars per line

- the hash function will be tested over all the words in the english language (>200000 words) and *must* achieve fewer than 30 collisions

Exemple