

Validate it

Descriere

AcadNet 2021

Author: Alexandru Razvan Caciulescu

Welcome to the "Validate it" challenge!

Perhaps the most important aspect of a blockchain is the ability to check and guarantee its integrity. Now that you have a new found understanding of crypto and its inner working you want to test its credibility and attempt to craft an attack that changes the transaction value of the 3rd to last block to contain the value "ACADNET BLOCKCHAIN RULLZ 2021!" AND also pass the block (node) validity test. Don't worry if it fails the chain validity test, after all, no one hacked the world in a day.

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

- upload a text file that contains at most 2 lines of code that will be placed in the marked location in `blockchain.c`.
- neither line can have more than 160 characters.
- the correct output should be *similar* to the output example. (it won't be exactly the same due to the random number generator)

Exemple

Exemplul 1

Intrare

Iesire

Is chain valid? false

Print chain

=====

Block data Let there be BitCoin ! \$\$\$

Block hash 18446744072750972478

Block previous hash 0

Block validity true

Block data Transaction 0, payload: 1736636756

Block hash 927646235

Block previous hash 18446744072750972478

Block validity true

Block data Transaction 1, payload: 1967847744

Block hash 433726464

Block previous hash 927646235

Block validity true

Block data Transaction 2, payload: 2073621153

Block hash 239559819

Block previous hash 433726464

Block validity true

Block data Transaction 3, payload: 170509073

Block hash 455687593

Block previous hash 239559819

Block validity true

Block data Transaction 4, payload: 679311451

Block hash 1874189837

Block previous hash 455687593

Block validity true

Block data Transaction 5, payload: 1269986938

Block hash 2317407130

Block previous hash 1874189837

Block validity true

Block data Transaction 6, payload: 1907454046

Block hash 389963891

Block previous hash 2317407130

Block validity true

Block data Transaction 7, payload: 591142252

Block hash 1454620468

Block previous hash 389963891

Block validity true

Block data Transaction 8, payload: 1362950186

Block hash 579774256

Block previous hash 1454620468

Block validity true

Block data Transaction 9, payload: 1690138556

Block hash 18446744073014554512

Block previous hash 579774256

Block validity true

Block data Transaction 10, payload: 908311834

Block hash 18446744071633251585

Block previous hash 18446744073014554512

Block validity true

Block data Transaction 11, payload: 93105267

Block hash 18446744073277385439

Block previous hash 18446744071633251585
Block validity true

Block data Transaction 12, payload: 317045969
Block hash 328766777
Block previous hash 18446744073277385439
Block validity true

Block data Transaction 13, payload: 1662614707
Block hash 1332216192
Block previous hash 328766777
Block validity true

Block data Transaction 14, payload: 867485515
Block hash 204550433
Block previous hash 1332216192
Block validity true

Block data Transaction 15, payload: 1230200953
Block hash 18446744073495941915
Block previous hash 204550433
Block validity true

Block data Transaction 16, payload: 1059176220
Block hash 18446744073433241918
Block previous hash 18446744073495941915
Block validity true

Block data ACADNET BLOCKCHAIN RULLZ 2021!
Block hash 18446744071354528896
Block previous hash 18446744073433241918
Block validity true

Block data Transaction 18, payload: 83781823
Block hash 846797053
Block previous hash 122819576
Block validity true

Block data Transaction 19, payload: 745977159
Block hash 2837926856
Block previous hash 846797053
Block validity true