

Work on project. Stage 5/6: Matters of security

30 users solved this problem. Latest completion was about 12 hours ago.

Project: [Blockchain](#)

Medium 16 minutes ?

§1. Description

How safe is your messaging system at the moment? Anyone can add a message to the blockchain. But can anyone impersonate you and send a message using your name? Without encryption, this is totally possible. There needs to be a method to verify that it is actually you who sent this message. Note that the registration/authorization method is bad because there is no server to check for a valid login/password pair. And if there is, it can be cracked by the hackers who can steal your password. There needs to be a whole new level of security.

Asymmetric cryptography solves this problem. With this, you can sign the message and let the signature be a special part of the message. You can generate a pair of keys: a public key and a private key. The message should be signed with a private key. And anyone can verify that the message and the signature pair is valid using a public key. The private key should be only on your computer, so no one from the internet can steal it. If you think that someone can steal your computer to get the private key, you can delete it from the computer and keep it in your head—that would be an example of maximum safety!

Please take a look at <http://www.mkyong.com/java/java-digital-signatures-example/> for code examples for creating private and public keys and signing and verifying the message.

Now there is another problem. A hacker can't just take any message and sign it like it is your message, but he can take an already signed message and paste it into the blockchain again; the signature of this message stays the same, doesn't it? For this reason, all messages should contain a unique identifier, and all these identifiers should be in ascending order in the blockchain.

To get a unique identifier you should implement a method in the Blockchain class that always returns different numbers in the ascending order starting from number 1.

In this stage, you need to upgrade the messages. The message should include the text of the message, the signature of this message, a unique identifier (remember to include a unique identifier when creating a signature), and a public key so everyone can check that this message is valid. Don't forget to check every message when checking that the blockchain is valid! The blockchain should reject the messages with identifier less than maximum identifier in the block in which miners looking for the magic number. Also, when validating the blockchain you should check that every message has an identifier greater than the maximum identifier of the previous block.

§2. Output example

Output is the same as in the previous stage, but with the exception that no one can impersonate you and create a message using your name. To be tested successfully, program should output information about first five blocks of the blockchain. Blocks should be separated by an empty line.

```
Block:
Created by miner # 9
Id: 1
Timestamp: 1539866031047
Magic number: 34729843
Hash of the previous block:
0
Hash of the block:
1d12cbbb5bfa278734285d261051f5484807120032cf6adcca5b9a3dbf0e7bb3
Block data:
Tom: Hey, I'm first!
Block was generating for 0 seconds
N was increased to 1

Block:
Created by miner # 7
Id: 2
Timestamp: 1539866031062
Magic number: 45389457
Hash of the previous block:
1d12cbbb5bfa278734285d261051f5484807120032cf6adcca5b9a3dbf0e7bb3
Hash of the block:
04a6735424357bf9af5a1467f8335e9427af714c0fb138595226d53beca5a05e
Block data:
Tom: Hey, I'm second also!
Block was generating for 0 seconds
N was increased to 2

Block:
Created by miner # 1
Id: 3
Timestamp: 1539866031063
Magic number: 24234687
Hash of the previous block:
04a6735424357bf9af5a1467f8335e9427af714c0fb138595226d53beca5a05e
Hash of the block:
0061924d48d5ce30e97cfc4297f3a40bc94dfac6af42d7bf366d236007c0b9d3
Block data:
Sarah: It's not fair!
Sarah: You always will be first because it is your blockchain!
Sarah: Anyway, thank you for this amazing chat.
Block was generating for 0 seconds
N was increased to 3

Block:
Created by miner # 2
Id: 4
Timestamp: 1539866256729
Magic number: 12376812
Hash of the previous block:
0061924d48d5ce30e97cfc4297f3a40bc94dfac6af42d7bf366d236007c0b9d3
Hash of the block:
000856a20d767fbbc38e0569354400c1750381100984a09a5d8b1cdf09b0bab6
Block data:
Tom: You're welcome :)
Nick: Hey Tom, nice chat
Block was generating for 5 seconds
N was increased to 4
```

[Code Editor](#)

[IDE](#), + 💎 100


Start using IDE! Get 💎 100 for the first problem solved via IDE



✓ IDE is responding IntelliJ IDEA 2017.3.7

✖ **Plugin IS NOT responding**

You may need to [install and configure it.](#)

 Show discussion (0)