Criptografia i Seguretat [104355]

Activitat Blockchain

1. Connect to the following URL:
   Group 81:
   `https://deic.uab.cat/~cborrego/block-81/doc.php`
   Group 82:
   `https://deic.uab.cat/~cborrego/block-82/doc.php`
   and read the Blockchain Documentation.
2. Generate a pair of public/private keys using the **Create Keys** link located on the website header. Do not lose them, otherwise you will not be able to prove your work.
3. **First block** to create and mine: Say hello to the world using a *Format-free Data*, as explained in Section 4. For example, create a block with the following Data field:

   `[Hola, amigos de la blockchain! :)]`
4. **Second block** to create and mine: Create a block with a **signed** *Assignation Data*, as in Section 1. You should write in the blockchain the following statement:

   `[NIU=mark]`

   where NIU is your NIU and mark the mark you will get for this assignment. For signing your data you can use the **Sign** link located on the website header.
5. How do you thing the signature is calculated?
6. In the **Verify** link located on the website header you can verify a signature for a given text and public key. How do you think this signature is verified?
7. **Third block** to create and mine: Get some easy money by mining the blockchain and generating Coin as explained in Section 3 from the Documentation.
8. **Fourth block** to create and mine: Pay your dues! Transfer the money you have created to your best friend using a Currency Transfer Block, as explained in Section 2 from the Documentation.
9. **Generate a script** to mine at the speed of light. You can use python by doing something similar to this:
   Group 811:

```python
import requests
pload = {'variable1':'value1','variable2':'value2'}
r = requests.post('https://deic.uab.cat/~cborrego/block-81/block.php',data = pload)
print(r.text)
```

   Group 812:

```python
import requests
pload = {'variable1':'value1','variable2':'value2'}
r = requests.post('https://deic.uab.cat/~cborrego/block-82/block.php',data = pload)
print(r.text)
```

   Additionally, you can also use *curl* in a Linux terminal by doing something similar to this:
   Group 811:

```
curl -d "variable1=value1&variable2=value2" -X POST https://deic.uab.cat/~cborrego/block-81/block.php
```

   Group 812:

```
curl -d "variable1=value1&variable2=value2" -X POST https://deic.uab.cat/~cborrego/block-82/block.php
```

10. Use your script to mine some blocks to make some money.
11. Prepare yourself: Richest miner wins some Sugus. :)
12. Additional prize: poorest miner wins also some Sugus! :)