Health Ledger Using Blockchain

User instructions

When program is run, users can select numbers to:

1.Create profile
2.View profile
3.Update profile
4.View other's profile
0.Exit program

<u>**Option 1**: Create profile</u>

The option creates profile of user’s medical data.
The user is asked to enter his details. The details are then converted into a SHA256 hexadecimal string, which is mined.
After block is successfully mined, user receives his private key. And the block is added to chain.

<u>**Option 2**: View profile</u>

The option lets user view his profile data.
The user is asked to enter his private key. The private key is verified and user details are made available.

<u>**Option 3**: Update profile</u>

The option lets user update his data.
The user is asked to enter his private key. If key is valid, then user is asked if he chooses to update a specific field. After updating the required fields, the block is mined and a new private key is displayed to the user. A new block is now added to the chain.
User only has to remember the latest displayed key.

<u>**Option 4**: View other's profile</u>

The option lets user view the other user’s (patient) data.
The user is asked to enter the patient’s SHA256 encrypted name. If valid key is entered, he is asked to enter his name. If the entered name of the user is listed in patient’s permitted users, then zero knowledge proof is started to further verify the transaction.

Zero knowledge proof has two people – prover and verifier – to prove that the user has the patient’s encrypted name. This is proved by executing a probability based algorithm, by taking inputs from both prover and verifier.

The prover is asked to enter a large prime number. Then prover is asked to enter a random number between 2 and prime number-1.
The verifier then is asked to enter a boolean (0/1) value. The verifier then matches the values and gives user access to the medical details of the patient.

<u>**Option 0**: Exit program</u>

The option lets the user exit the ledger.
Note: All previous data will be erased on choosing this option.