# Tema - Bitcoin minning

#### Informatii:

- Tema se realizeaza individual;
- Tema presupune gasirea valorii hash corespunzatoare unui bloc minat in Bitcoin, care satisfice dificultatea ceruta; Mai exact:

Puteti gasi nonce-ul pentru care valoarea hash verifica dificultatea ceruta (i.e., incepe cu cel putin ... cifre 0)?

Altfel spus, testam dificultatea minarii unui bloc, atunci cand se stie ca blocul respectiv poate fi minat. In practica, problema este si mai dificila, pentru ca nu mereu exista o valoare nonce care sa satisfaca cerinta fara a se modifica componenta blocului, mai exact Merke root sau timpul. Pentru tema, o astfel de valoare nonce exista.

- Mai multe despre Bitcoin si link-uri care pot fi de ajutor pentru rezolvarea temei:
  - o [1] https://en.bitcoin.it/wiki/Main Page
  - [2] S.Nakamoto, Bitcoin: A Peer-to-Peer Electroic Cash System https://bitcoin.org/bitcoin.pdf
  - [3] Ken Shirriff's blog: Bitcoin mining the hard way: the algorithms, protocols, and bytes
     http://www.righto.com/2014/02/bitcoin-mining-hard-way-algorithms.html
  - [4] Bitcoin explorer: https://btc.com/

## Pasi de urmat:

- Cititi despre cum se publica un bloc / se obtine valoarea hash a unui bloc de o anumita dificultate, adica incepe cu un anumit numar de cifre 0. Mai exact, pentru calculul valorii hash se folosesc versiunea protocolului (Version), valoarea hash a blocului anterior (Prev Block), valoarea Merkle root (Merke Root), timpul la care s-a minat blocul respectiv (Time), dificultatea impusa (conform campului Bits). Denumirile indicate in paranteza sunt numele campurilor, asa cum le gasiti in [4].
- Scrieti o secventa de cod sau modificati codul existent online [3] pentru calculul valorii hash pornind de la campurile mentionate mai sus, pentru valorile:
  - Version: 0x20400000
  - Prev Block:
    00000000000000000006a4a234288a44e715275f1775b77b2fddb6c02
    eb6b72f
  - Merkle Root:
    2dc60c563da5368e0668b81bc4d8dd369639a1134f68e425a9a74e42 8801e5b8
  - Time: 0x5DB8AB5E

o Bits: 0x17148EDF

Pentru verificarea secventei de cod, puteti folosi valorile:

Version: 0x3fff0000

Prev Block:
 000000000000000000140ac4688aea45aacbe7caf6aaca46f16acd93e
 1064c3

 Merkle Root: 422458fced12693312058f6ee4ada19f6df8b29d8cac425c12f4722e0dc4

Time: 0x5E664C76Bits: 0x17110119

Nonce1: 538463288 (0x20184C38)

Acestea corespund blocului cu height = 620954.

Alternativ, puteti prelua oricate cazuri de test din blocurile publicate [4].

- Trebuie sa rulati codul in 2 cazuri:
  - Valoarea nonce se initializeaza de la 3 000 000 000, caz in care trebuie sa gasiti o valoare nonce1 mai mica decat 3 100 000 000 pentru care se satisfice dificultatea, i.e., se gaseste o valoare hash care incepe cu numarul de zerouri cerut.
  - Valoarea nonce se initializeaza de la un numar aleator, dar mai mare decat valoarea nonce1 gasita anterior. Atentie! Nu valoarea imediat mai mare, i.e. nonce1 +1, ci un numar (pseudo-) aleator oarecare, cu conditia sa fie mai mare decat valoarea nonce1 gasita mai sus. Verificati pentru cel putin 100 000 000 de valori succesive pornind de la aceasta valoare, sau pana cand ati gasit un nonce2 pentru care valoarea functiei hash satisfice dificultatea.

## Date importante / termene limita:

• Transmiterea temelor: 22 aprilie, ora 23:55

#### Mod de transmitere al temelor:

- Temele trebuie transmise prin Moodle.
- Studentii care nu transmit tema pana la termenul limita pierd punctajul aferent acesteia.
- Temele se transmit prin Moodle conform cu specificatiile postate.
- Rezolvarea trebuie sa contina:
  - o Cazul 1:
    - Valoarea nonce1 gasita

- Valoarea hash a blocului care satisfice dificultatea, calculata din valorile date mai jos si nonce 1
- Primele 5 valori hash, corespunzatoare lui nonce = 3 000 000 000 ... 3 000 000 004.
- o Cazul 2:
  - Valoarea initiala nonce2 (valoarea pseudo-aleatoare de la care ati pornit)
  - Numarul de testari (cate valori nonce ati testat pornind de la nonce2 prin incrementare)
  - Am gasit o valoare hash care satisfice dificultatea in cazul 2: DA/NU
  - Daca DA: nonce2 si valoarea hash
- Codul sursa pentru rezolvarea temei (raw sau link catre cod)

# Exemplu de raspuns (pastrati aceeasi structura si denumirile campurilor):

#### Cazul 1:

- Nonce1: 538463288 (0x20184C38);
- o Block Hash: 000000000000000000d493c3c1b91c8059c6b0838e7e68fbcf8f838260 6b82c:
- o Primele 5 valori hash (in acest caz pentru nonce 0..4, in tema pentru 3 000 000 000 ... 3 000 000 004):
  - f8d6a428731b3a30a28b46bf7bf3baea848c349a5a48b1eb740bc 667c2f31a58
  - 992111328ec08d817c2668549ae44e5e0a43a9b6e43230f9f67f7 cd4e9738fec
  - 88acbda554a28699db7ddb763034ef3a28cf24cf5280fab4f2ddb0 8268db3937
  - 66bab3a5e2f2c80b475baa96ad1ebb582b76ca50ea18c361c60e 49eec6d9fd46
  - 19a634b81721f64bc8e425c37b3106518a03152dd01fae4ec6479 25bd3081a54

#### Cazul 2:

 Nonce2 start: 1531678903 Numar testari: 100 000 000

Succes: NU

Nonce2: - (se completeaza numai daca Succes: DA)

Hash2: - (se completeaza numai daca Succes: DA)

Codul sursa: <cod sursa - raw sau link catre cod>

#### Criterii de notare:

- Transmiterea temei:
- Transmiterea tuturor informatiilor cerute;
- Transmiterea informatiei in formatul cerut.