CYBER SECURITY

5. forduló

A kategória támogatója: Continental

Ismertető a feladatlaphoz

> Kezdj neki minél hamarabb, mert a feladatot a forduló záró időpontjáig lehet beküldeni, nem addig lehet elkezdeni!

Sok sikert!

Az ötödik fordulóban szintén egy olyan feladattal jelentkezünk, melyhez hasonlóval tavaly is találkozhattak már, akik részt vettek a versenyen.

A blokklánc (angolul blockchain) egy olyan decentralizált adatbázis, ahol különböző, akár ellenérdekelt felek tudnak hitelesen, megbízhatóan tranzakciókat végrehajtani hamisítást kizáró módon. Működés során egy egyre bővülő, megváltoztathatatlan log készül minden egyes tranzakció után, amik egy-egy adatblokkot alkotnak. Blokkláncok alkalmazása többek között kriptovaluták terén létfontosságúak.

Mivel nincs központi ellenőrző rendszer, kiemelt szerepet kap a rendszerben a hitelesítés.
Blokkláncok terén egy speciális kiszűrendő hiba az úgynevezett bizánci hiba.
Bizánci hiba egy olyan típusú meghibásodás, ahol a hálózat egy eleme különböző információt továbbít a többiek felé. Az elnevezés a bizánci tábornokok problémájáról keletkezett:

Tegyük fel „n” darab bizánci sereg körbekerít egy ellenséges erődítményt. A tábornokok tanácskoznak maguk között, hogy rohamozzanak-e aznap este, vagy másnapra halasszák a rohamot. Sajnos árulók vannak a berkeikben, akiknek céljuk a többiek összezavarása. A tábornokok személyesen nem találkozhatnak, csak futárok által üzenhetnek egymásnak. Korábbi megbeszélés alapján a többség döntése alapján fognak cselekedni, hiszen akár támad-

nak, akár (ideiglenesen) visszavonulnak, az a céljuk, hogy egységesek maradjanak, ha a hűséges seregek egyik fele támad, a maradék visszavonul, akkor a csata elveszik.

Indítás utáni csatolmányok

1. feladat 20 pont

Tegyük fel, hogy a 11 tábornokunk értesül arról, hogy pontosan 2 áruló van maguk között. Ebből az információból kiindulva, elkérik egymástól levélben nem csak azt, hogy mi a döntésük, de azt is, hogy a többi tábornoktól ki mit hallott.

Továbbá új feltevésként vegyük úgy, hogy az ostromlott város tökéletes kémekkel rendelkezik, akik a különböző táborokba belopakodnak, és fültanúi lesznek minden támadási / visszavonulási szándéknak, illetve a tábornokok egymásnak küldött üzeneteik tartalmának. A megszerzett információt továbbítják a városba, ahol az alábbi formában összesítik az adatokat a kémfőnök számára, amiket a csatolt Bizanci_tabornokok.txt fájl tartalmaz:

· D[i][i][i] = i. tábornok saját döntése, amit ha hűséges, akkor ő csak ezt továbbítja tábornok társainak (i=0…10)

· D[i][i][j] = i.-ik tábornok milyen üzenetet kapott, j.-ik tábornok szándékáról (i!=j, i, j=0...10)

D[i][j][k] =i.-ik tábornok j-iktől mit hallott k-ik döntéséről (i,j,k=0…10, páronként különbözőek)

Hogyan fognak dönteni a (nem áruló) tábornokok, ha feltételezzük, hogy tökéletesen dolgozzák fel a rendelkezésükre álló információkat?

A) Minden hű tábornok támadni fog

B) Minden hű tábornok vissza fog vonulni

C) Nem fognak egységesen dönteni a hű tábornokok

Válasz

- ○ A
- ○ B
- ○ C

2. feladat 20 pont

Állapítsuk meg, hogy a rendelkezésre álló információból az árulók személyazonossága (indexe) ki számára lesz ismert!

A) Minden hű tábornok és a kémfőnök is fogja tudni, kik az árulók

B) Csak néhány hű tábornok és a kémfőnök fogja tudni, kik az árulók

C) Csak a város kémfőnöke fogja tudni, kik az árulók

D) Semelyik fél számára nem megállapítható, kik az árulók

Válaszok

- [ ] A
- [ ] B
- [ ] C
- [ ] D

Megoldások beküldése