מטלה 11 - ביטקוין - פתרון

שאלה 1: חלוקה הוגנת במועדון כריה

לאחר כמה ניסיונות כושלים לכרות בלוקים של ביטקוין בעזרת הסמארטפון שלכם, החלטתם להקים מועדון כריה (mining pool). פרסמתם מודעה באינטרנט, אספתם כמה כורים והסכמתם לכרות בלוקים ביחד. סיכמתם ביניכם, שהראשון שיצליח לכרות בלוק - יתחלק בדמי-הכריה עם כולם.

התרומות של חברי המועדון לא שוות - לכל אחד יש חומרה אחרת, כל אחד משקיע זמן אחר בכריה וכו'. אתם רוצים לחלק את דמי-הכריה של כל בלוק באופן יחסי לכמות העבודה שכל אחד השקיע.

מיצאו שיטה לחישוב כמות העבודה שהשקיע כל כורה בכריית בלוק נתון. פרטו והדגימו את השיטה.

- **פתרון**: במחשבה ראשונה אפשר לחשוב שצריך למדוד את איכות החומרה של כל כורה במועדון, כמה זמן כל כורה השקיע וכו', אבל זה לא יעבוד. גם אם מישהו מוכיח לנו שהוא קנה חומרה מאד יקרה, מי אמר שהוא בכלל משתמש בה? ייתכן שהוא קנה אותה ושם בבוידעם (כדי לחסוך חשמל)... גם אם מישהו מביא חשבון חשמל המוכיח שהוא השתמש בחומרה שלו, מי אמר שהוא באמת השתמש בה לכריה ולא למשהו אחר, למשל לעיבודים גרפיים (אם החומרה היא *GPU*)?
- אבל, אנחנו כבר מכירים דרך שבה אפשר להוכיח עבודה (*Proof of Work*) - מציאת ערך *nonce* שיגרום ל-*hash* של הבלוק להיות קטן ממספר מסויים המבטא את רמת הקושי. אם כן, כדי לוודא שהכורים אכן עובדים, צריך לבקש מהם לשלוח ערכי *nonce* עם רמת קושי נמוכה יותר. לדוגמה, נניח שכדי לכרות בלוק שלם, צריך שההאש יהיה קטן מ-1000. אז, המועדון יכול לבקש מכל כורה למצוא ערכי האש קטנים מ-100,000. כל כורה שימצא האש כזה, יקבל 1% מהתשלום על הבלוק, כי בממוצע הוא עשה 1% מהעבודה. כדי להגיע לרמת דיוק גבוהה יותר אפשר להקטין עוד יותר את רמת הקושי, למשל כל כורה שמצא האש קטן מ 1,000,000 יקבל אלפית מהתשלום על הבלוק, וכו'.

שאלה 2: קביעת רמת הקושי

לצורך השאלה, הניחו שקיימת המחלקה הבאה, המייצגת בלוק בשרשרת-הבלוקים:

```
struct Block {
     //... more methods
      long timestamp();    // time of block creation; seconds since 1/1/2008
     double difficulty();   // level of difficulty in block creation time.
     Block* previous();  // the preceding block in the chain.
     //... more methods
};
```

רמת הקושי של כריית בלוק צריכה להתעדכן בערך פעם בשבועיים. כיתבו פונקציה שאפשר להריץ פעם בשבועיים על-מנת להעריך את רמת הקושי הדרושה על-מנת שבלוק ייווצר בממוצע כל 10 דקות.

הפונקציה מקבלת קישור לבלוק האחרון בשרשרת, ומחשבת את רמת הקושי הדרושה בהתאם לקצב היצירה של הבלוקים מהשבועיים האחרונים. היעזרו בנוסחה הבאה, המחשבת את קצב היצירה הצפוי לפי רמת הקושי:

https://en.bitcoin.it/wiki/Difficulty#How_soon_might_I_expect_to_generate_a_block.3F

פתרון: הזמן הדרוש ליצירת בלוק (T) שווה לרמת הקושי (D) כפול קבוע כלשהו (C):

$$T = D*C$$

במשך שבועיים צריכים להיווצר כ-2016 בלוקים (14 ימים כפול 144 בלוקים ליום). לכן, דרך פשוטה לחישוב רמת הקושי היא:

- א. לחשב כמה זמן לקח ליצור את 2016 הבלוקים האחרונים ($T0$).
- ב. לקרוא מהבלוק את רמת הקושי האחרונה ($D0$).
- ג. בהתאם לנוסחה למעלה, לחשב את הקבוע $C = T0/D0$
- ד. הזמן הרצוי ליצירת 2016 בלוקים הוא שבועיים: $T1=14*86400$
- ה. מכאן, רמת הקושי החדשה היא:

$$D1 = T1/C = (T1/T0)*D0$$

עכשיו נשאר רק לכתוב את הפונקציה:

```
double newDifficulty(Block* lastBlock) {
     // a. calculate how much it took to create last 2016 blocks:
     long now = lastBlock->timestamp();
     for (int i=0, Block* b=lastBlock; i<2016; ++i)
          b = b->previous();
     long then = b->timestamp();
     long T0 = now-then;   // in seconds

     // b. read the most recent difficulty:
     long D0 = lastBlock->difficulty();

     // c. calculate the required time:
     long T1 = 14*86400;    // num of seconds in two weeks
     return (T1/T0)*D0;
}
```

שאלה 3: ביטקוין ירוק

קיראו על Bitcoin Green באתר זה: https://www.savebitcoin.io והסבירו:

א. מהי הבעיה הסביבתית שנוצרת ע"י ביטקוין, ומהו הפתרון שמציעים יוזמי Bitcoin Green?

ב. מה ההבדל בין Proof-of-Stake לבין Proof-of-work, ומה הקשר לסעיף הקודם?

- **פתרון**: ראו בפתרונות של מירב ונעמה, רז ואורן, ניסן ואריה.

שאלה 4: ארנקים ועסקאות - תרגיל מעשי

א. הורידו והתקינו ארנק ביטקוין התומך ברשת-ניסוי, למשל BitPay: https://github.com/bitpay/copay/releases/tag/v4.3.6

ב. צרו ארנק חדש, והקפידו לבחור באפשרויות המתקדמות (advanced) את "רשת הניסוי" - TestNet.

ג. השיגו ביטקוין-ניסוי מאחד הברזים, למשל כאן: https://testnet.manu.backend.hamburg/faucet

ד. שילחו חלק מהביטקוין שקיבלתם לצוות אחר בכיתה.

ה. מיצאו את הבלוק שלכם בשרשרת הבלוקים של רשת הניסוי: https://testnet.blockchain.info

כפתרון לשאלה, צרפו צילום מסך המראה בבירור את הבלוק עם העיסקה שעשיתם.

שאלה 5: איזה כורה זוכה בבלוק?

נניח שברשת ביטקוין ישנם חמישה כורים. יעילות הכריה היחסית שלהם באחוזים היא: 30, 25, 20, 15, 10.

א. תארו אלגוריתם-כריה, שאם כל הכורים יממשו אותו - הכורה הראשון (30) יזכה בכל הבלוקים והאחרים לא יזכו בכלל.

ב. תארו אלגוריתם-כריה אחר, שאם הכורה האחרון (10) יממש אותו - הוא יזכה בממוצע ב-10% מהבלוקים, לא משנה מה יעשו האחרים.

- **פתרון**: ראו בפתרון של אוריאל ויואב.

שאלה 6: מתקפת פיני (על-שם Hal Finney שחשב עליה ראשון)

נניח שמישהו, נקרא לו "התוקף", רוצה להשתמש במטבע אחד פעמיים. הוא פועל לפי האלגוריתם הבא. הוא כורה בלוקים באופן רגיל; בכל בלוק שהוא כורה, כאחת מ-2000 העיסקאות בבלוק, הוא מכניס עיסקה אחת של מטבע א מכתובת ב לכתובת ג, כאשר שתי הכתובות שייכות לו. ברגע שהוא מצא בלוק, במקום לפרסם אותו מייד, הוא הולך לחנות, קונה חפץ ומשלם עליו במטבע א מכתובת ב לכתובת של המוכר. ברגע שהוא יוצא מהחנות, הוא שולח את הבלוק המאושר שמצא בצעד הראשון. הבלוק מאושר, העיסקה שעשה עם המוכר נדחית, המוכר מפסיד את הכסף, והתוקף קיבל חפץ בלי לשלם.

א. מה הסיכון שהתוקף לוקח? באיזה מקרה ההתקפה תיכשל, וכמה יפסיד התוקף במקרה זה?

- **פתרון**: התוקף כבר מצא בלוק הממשיך את הבלוק הקודם, ויכל לפרסם אותו מייד ולקבל 12.5 ביטקוין. אם, בזמן שהתוקף נמצא בחנות ומחכה למוכר, מישהו אחר ימצא בלוק הממשיך את הבלוק

הקודם ויפרסם אותו, אז הבלוק שהתוקף מצא לא יתקבל, והוא יפסיד 12.5 ביטקוין - בערך 100 אלף דולר.

ב. המוכר מחכה t דקות לפני מסירת החפץ. מה צריך להיות ערך החפץ כך שההתקפה תהיה כדאית?

- הסיכוי שמישהו ימצא בלוק אחר, הממשיך את הבלוק הקודם, תוך t דקות, הוא בערך $t/10$. לכן, תוחלת ההפסד של התוקף (בביטקוין) היא: $t*12.5/10 = t*1.25$.
- ההתקפה כדאית אם ורק אם ערך החפץ הוא יותר מ $t*1.25$ ביטקוין (במחירים של היום: בערך 10,000 דולר לדקה).

ג. מה יכול המוכר לעשות כדי להגן על עצמו מהתקפה זו?

- **פתרון**: המוכר יכול פשוט לחכות כ-10 דקות, עד שיראה שהעיסקה שלו אושרה בבלוק שחובר לשרשרת. במקרה זה ההתקפה נכשלת בוודאות.
- אם הוא לא רוצה לחכות 10 דקות (כי יש תור ארוך), הוא יכול לחכות קצת יותר מ-$V/1.25$ דקות, כאשר V הוא ערך החפץ בביטקוין; כפי שהסברנו למעלה, במקרה זה ההתקפה לא משתלמת.
לדוגמה, אם הוא מוכר חפץ ששווה 1/48 ביטקוין (כ-150 דולר) או פחות, מספיק שיחכה שניה אחת.