מטלה 11 - ביטקוין - טיוטה

יש לענות על שאלה אחת לבחירתכם. הגשה בזוגות, עד תחילת ההרצאה הבאה.

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.

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

כותרת הפונקציה שאתם צריכים לממש:

```
double newDifficulty(Block* lastBlock);
```

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?

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 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.

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?

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

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