מטלה - אתריום

יש לענות על שאלה אחת לבחירתכם.

שאלה 1: אבן נייר ומספריים עם סודיות

א. ודאו שאתם יכולים לקמפל ולהריץ את החוזה של "אבן נייר ומספריים" שהוצג בכיתה (בקובץ code/rps.sol) בסביבת רמיקס: https://remix.ethereum.org (אמור לעבוד בדפדפן Chrome).

ב. שנו את התוכנית בהתאם למה שנלמד בהרצאה, כך שהבחירות של שני השחקנים יישמרו בסוד עד לסיום המשחק, ולא יהיה אפשר לראות אותן דרך שרשרת הבלוקים.

שאלה 2: משאל עם

כיתבו חוזה חכם בשפת solidity המאפשר לבצע משאל-עם. למשאל יש שתי תוצאות אפשריות: "כן" (1) או "לא" (0). החוזה יתמוך בפעולות הבאות:

- addVoter – הוספת כתובת ציבורית של אזרח שיש לו זכות בחירה. שיטה זו ניתנת להרצה רק ע"י מי שיצר את החוזה.
- vote – הצבעה – 0 או 1. שיטה זו ניתנת להרצה רק ע"י אזרח שנוסף לפני-כן לחוזה ע"י addVoter. כל אזרח יכול להצביע רק פעם אחת לכל היותר.
- outcome – שיטה המחזירה את תוצאת המשאל – 0 או 1.

שאלה 3: מכרז

כיתבו חוזה חכם בשפת solidity המאפשר לבצע מכרז מחיר שני. בהתחלה המכרז הוא ב"בעלות" מי שיצר את החוזה; בכל פעם שמישהו זוכה במכרז, המכרז עובר לבעלותו. החוזה יתמוך בפעולות הבאות:

- bid – שליחת כסף לחוזה לצורך השתתפות במכרז. ההכרזה שווה לכמות הכסף שנשלח.
- conclude – סיום המכרז הנוכחי. שיטה זו ניתנת להרצה רק ע"י הבעלים הנוכחי של המכרז. השיטה מבצעת את הפעולות הבאות: (1) חישוב הזוכה – זה ששלח הכי הרבה כסף דרך bid. (2) החזרת הכסף לכל המשתתפים שלא זכו. (3) החזרת חלק מהכסף לזוכה – ההפרש בין המחיר שלו לבין המחיר השני. (4) העברת המחיר השני לבעלים הנוכחי של החוזה. (5) שינוי כתובת ה"בעלים" של החוזה לכתובתו של הזוכה – כך שהזוכה הופך להיות הבעלים החדש של החוזה.

שאלה 4. חוזה חכם לפתרון בעיה NP-שלמה

ב**בעיית חלוקת המספרים**, נתון מערך של מספרים שלמים. צריך לחלק אותו לשני תת-מערכים, כך שסכום המספרים בשני המערכים הוא זהה (בהנחה שאכן קיימת חלוקה כזאת).

למשל: אם הקלט הוא המערך {1,2,3,4}, אז פלט אפשרי הוא שני המערכים: {1,4} ו {2,3}.

כיוון שהבעיה היא קשה חישובית, אנחנו רוצים לכתוב חוזה חכם במערכת אתריום, שיעודד אנשים לפתור את הבעיה בעצמם ויתן פרס של 1 אֶתֶר לפותר הראשון.

לפניכם שלד של חוזה בשפת solidity (להזכירכם, int[] הוא מערך של מספרים שלמים, כמו ב-Java):

```
contract Partition {
    constructor(int[] input) public {
         ....
    }

    function solve(int[] part1, int[] part2) public {
         ....
    }
}
```

- הבנאי של החוזה מקבל כקלט את המערך שיש לחלק.
- הפונקציה solve היא הפונקציה שהפותרים צריכים לקרוא לה כדי להציע את הפתרון שלהם לבדיקה.

השלימו את שתי הפונקציות החסרות. הוסיפו משתנים ופונקציות נוספים לפי הצורך.

אם אינכם זוכרים את התחביר של שפת solidity, הניחו שהתחביר זהה לשפת Java או C++ לפי בחירתכם. כמו כן, אתם יכולים להשתמש בכל הפונקציות הנמצאות בספריות התקניות של השפות הללו. הסבירו היטב בעברית מה אתם עושים.