

מטלה 12 - אתריום

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

שאלה 1: אבן נייר ומספריים עם בחירות סודיות

א. ודאו שאתם יכולים לקמפל ולהריץ את החוזה של "אבן נייר ומספריים" שהוצג בכיתה (בקובץ smart contracts/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: שימוש ברשת אתריום לפתרון בעיות NP שלמות

תזכורת: בעיה NP-שלמה היא בעיה עם המאפיינים הבאים:

- לא קיים (כנראה) אלגוריתם הפותר את הבעיה בזמן פולינומיאלי.
 - אם משהו כבר מביא לנו פתרון של הבעיה, אפשר לוודא בזמן פולינומיאלי שהפתרון נכון.
- א. נניח שאתם רוצים לפתור בעיה NP-שלמה כלשהי. אתם רוצים לשכנע אנשים שיעזרו לכם לפתור את הבעיה, ומציעים פרס לראשון שיפתור את הבעיה. הסבירו איך אפשר להשתמש לשם-כך בחוזה חכם.
- ב. בחרו בעיה NP-שלמה כלשהי וכתבו בשפת solidity חוזה חכם המממש את השיטה שתיארתם בסעיף א.