אתריום וחוזים חכמים
Ethereum and Smart Contracts

אראל סגל-הלוי

מקורות:

Ethereum White Paper / Vitalik Buterin, 2015

Smart Contracts: The Technology that will Replace Lawyers

שרשראות בלוקים

המצאת הביטקוין הביאה לעולם שני חידושים:

- מטבע מבוזר – לא תלוי בממשלה או בבנק.
- הסכמה מבוזרת על סדר-אירועים.

בעבר התלהבו בעיקר מהחידוש הראשון;

היום מתלהבים יותר מהחידוש השני. שרשרת הבלוקים מאפשרת להסכים על אירועים ולבצע פעולות רבות שאינן קשורות דווקא למטבעות.

זה הרעיון מאחרי מערכת **אתריום** (Ethereum).

חוזים חכמים

- כיום, כדי לאכוף חוזה, דרוש גוף מרכזי.
- מערכת **אתריום** היא מערכת שבה אפשר לכתוב **חוזים חכמים** – חוזים ניתנים לתיכנות. המערכת תאכוף אוטומטית ע"י ביצוע הקוד.
- **דוגמה**: מכירת יצירת-אומנות במכרז מחיר ראשון.
  - כל משתתף שולח את הכסף לחוזה החכם.
  - החוזה מחשב מקסימום ומגלה מי הזוכה.
  - החוזה מחזיר את הכסף למפסידים.

מכרז כזה אכן יתקיים ב-20/6/2012!

חוזים חכמים

דוגמאות נוספות:

- משחקים על כסף - "אבן נייר ומספריים".
  - שני השחקנים מפקידים כסף ובוחרים פעולה;
  - החוזה מחליט מי מנצח ושולח את הכסף.
- ביטוח שער מטבע-חוץ.
  - אם השער עולה/יורד, הלקוח מקבל כסף מיידית.
- שכירת חדר ב AirBnB – עם מפתח דיגיטלי.
  - החוזה מקבל מפתח מהמשכיר וכסף מהשוכר;
  - החוזה שולח מפתח לשוכר וכסף למשכיר.

מכונת אתריום וירטואלית - EVM

- המושג הבסיסי - **חשבון** (accout):
  - חשבון בבעלות חיצונית (בד"כ בבעלות אדם) - Externally-Owned Account.
  - חשבון של חוזה – Contract account – מייצג חוזה חכם בתוך המערכת. כולל **קוד** ו**זיכרון**.
- לכל חשבון, חיצוני או חוזה, יש **יתרה** ו**כתובת**.
  - היתרה היא במטבע הנקרא **אתר** (Ether).
    - אתר = 1000 פיני (Finney) = 1e9 גיגה-ווי (gwei).
  - הכתובת מאפשרת לקבל **אתר** והודעות.

מכונת אתריום וירטואלית – מצב

ה**מצב** של ה-EVM, בכל רגע נתון, כולל את:

- היתרה של כל החשבונות במערכת;
- הקוד והזיכרון של כל החוזים החכמים.

המצב של ה-EVM נשמר בשרשרת הבלוקים.

כל **מי** המעוניין להשתתף ברשת אתריום, צריך להוריד את כל שרשרת הבלוקים, לבצע את כל הקוד, ולחשב את המצב הנוכחי של ה-EVM.

מי משלם את עלויות ההרצה של כל הקוד הזה?

מכונת אתריום וירטואלית – דלק

- כל פעולה שמריצה קוד, צורכת "דלק" (gas).
  - לכל פעולה בשפת EVM יש "צריכת דלק".
  - צריכת-דלק של עסקה = 21000.
  - צריכת-דלק של כל בייט נוסף בעסקה = 68.
- כשמשתמשים פעולה לביצוע, צריך להגדיר כמות דלק מקסימלית ותשלום לכל יחידת דלק.
  - מחיר-השוק של דלק כיום: 4 ג'ווי (ננו-אתר).
- כשהדלק נגמר – הביצוע נפסק.
  - היתרון: לולאה אינסופית לא תתקע את הרשת!

חוזים חכמים – איך מתחילים?

1) מתקינים תוכנת **ארנק** – תוכנה המנהלת מפתחות פרטיים וציבוריים, שולחת עיסקאות וכו' - למשל:

- *ארנק על המחשב המקומי – MyEtherWallet*
- *תוסף לדפדפן כרום - MetaMask*

2) פותחים חשבון אחד או יותר דרך הארנק.

- *חשבון = זוג מפתחות. נשמר מקומית בלבד!*

3) משיגים קצת אתר – למשל דרך "ברז" של רשת-ניסוי כלשהי.

חוזים חכמים – איך מתכנתים?

1) כותבים קוד בשפה ייעודית כלשהי כגון:

* **Solidity** – דמויית ג'אבה (ראו דוגמאות בתיקיה smart-contracts);
* **Serpent** – דמויית פייתון.

2) מקמפלים לשפת-המכונה של ה-EVM:

* על מחשב מקומי – solc – מסובך;
* בדפדפן – remix.ethereum.org – פשוט.

3) שולחים את החוזה המקומפל לרשת אתריום.

* דרך MetaMask – כמו כל עיסקה אחרת.
* מרגע שהחוזה נשלח – הוא לא ניתן לשינוי!

חוזים חכמים – איך מפעילים?

1) שולחים לכל המשתמשים את:

- *קוד-המקור של החוזה;*
- *הכתובת שבה החוזה נמצא ברשת.*

2) כל משתמש יכול דרך remix:

- לקמפל את החוזה;
- להתחבר לחוזה הקיים;
- להפעיל את השיטות הציבוריות של החוזה;
- לראות את המשתנים הציבוריים של החוזה.

3) החוזה יכול לצבור כסף ולשלם כסף.

חוזים חכמים – דוגמאות

1) hello1.sol:

- המילה contract – חוזה (כמו מחלקה).
- המילים function, public, pure, returns
- הסוג bytes32

2) hello2.sol:

- שדות, שיטות משנות, שיטות מסוג view
- הסוג string
- event, emit

אבן נייר ומספריים – rps.sol

משחק לשני שחקנים על שרשרת הבלוקים.

- שחקן א מגיע, משלם 100 פיני, ובוחר rock/paper/scissors.
- שחקן ב מגיע, משלם 100 פיני, ובוחר rock/paper/scissors.
- המנצח מקבל 180 פיני; החוזה מרויח 20.
- במקרה של תיקו, כל שחקן מקבל 90.
- במקרה של קלט לא חוקי, כל שחקן מקבל 80.

אבן נייר ומספריים – בעיות

בעיה א: שחקן 2 יכול לראות את בחירת שחקן 1!

- פתרון: להפוך את המשתנים לפרטיים (ברירת המחדל).

-- זה לא מספיק – כל המידע גלוי על השרשרת!

- פתרון מתקדם: להשתמש ב-hash.
  - שחקן 1 שולח SHA256(choice_1)
  - שחקן 2 שולח SHA256(choice_2)
  - שחקן j שולח choice_j.
  - החוזה מאמת שה-hash זהה לקלט הראשון.

אבן נייר ומספריים – תמריצים

בעיה ב: שחקן 2 רואה את הבחירה של שחקן 1, מבין שהפסיד, ואין לו מוטיבציה לשלוח את הבחירה שלו!

- פתרון: לתת "פרס ניחומים" למפסיד אם שלח תוך זמן סביר.
- הפרס צריך לכסות את מחיר הגז של השליחה.

חוזים חכמים - אתגרים

חוזים חכמים המסתמכים על אירועים חיצוניים צריכים לקבל מידע על העולם החיצון. למשל:

- חוזה ביטוח דירה – צריך לדעת אם הדירה נשרפה.
- חוזה השכרת דירה – צריך לדעת אם הדייר נכנס.

פתרונות:

- חיישנים חכמים עם חשבון באתריום.
- מנעולים חכמים.

חוזים חכמים - סיכום

הנושא בחזית המחקר.

- המון אתגרים:
  - אתגרי הנדסת תוכנה
  - אתגרי תמריצים
  - אתגרי חומרה
- המון אפשרויות