**עבודת בית ראשונה: 10 נקודות מהציון הסופי -בנית שלד רשת בלוקציין.**

עבודה ראשונה – בזוגות או ביחידים

**לשלוח את העבודה משתי החשבונות של המשתתפים (אם ישלח אחד למרות שיצויין על העבודה שתי שמות רק מייל המגיש יקבל ציון השני** **0)**

**העתקה תפסול את המעתיקים והמעותקים ל 0**

**כללי**

אפשר להתחיל דרך השימוש בקוד ה JavaScript שסופק בכיתה (מצורף - גם לינק למקור), מותר לממש בכל שפה אחרת כולל C# Java Python C++ ומה שיעלה על דעתכם .

אין צורך ב GUI.

שגיאות מדווחות יתקבלו בברכה ☺

מקורות הקוד שבנינו בכיתה:

מקור <https://github.com/Savjee/SavjeeCoin>

Bloom filter, Merkle tree שקף

P2P רשת קוד ושקף (אם רוצים לממש)

Segwit ראה שקף

מתוך דוגמת תיקון EIP 1559<https://macrobit.co.il/eip-1559/> ישום המטבע כדפלציוני – [שרפת עמלות הבסיס (עיסקה) מטבע](https://ultrasound.money/), עם עליות עיסקה

**מטלה:**

1. (20%) לצרף שקף מסביר:
2. שקף ראשון: שמות המבצעים.
   1. מטלות מומשו עם Known Bug.
   2. מטלות שלא מומשו.
3. שקף שני: הוראות התקנה והפעלה.
4. שאר השקפים: ראה סעיף ו .
5. שלד לוג של הדגמת כריה ואימות מפורט.
6. מטרה : הדגמת רשת p2p (אפשר להדגים בשרת אחד – שני קבצים המייצגים צומת קל ו-ארנק מלא ) עם שלושה צמתים אחד הוא – כורה **Full nodes**))

**Full nodes** מכיל שרשרת בלוקציין שכורה את העסקאות (הקובץ שרובו הגדרנו בכיתה), והן נאגרות בעץ מרקל, ומימוש bloom פילטר. שני הצמתים האחרים הם Wallet-SPV (Simplify Payment Verification) יוגדרו דרך קובץ JS נוסף .

1. **להקלת בדיקת העבודה, כל סעיף המצויין להלן יש להראות את הקוד על השקף + הסבר בהיר קצר.**
2. (80%)
   1. מימוש ספריית bloom filter.וקוד הדגמת חיפוש.
   2. מימוש ספריית Merkle tree , וקוד בצד ה full nodes.
   3. קוד בדיקת קיום\אי קיום עיסקה בצד הארנק הקל. והדגמת אימות טרנזקציה של עיסקה ב - Wallet-SPV. או חוסר קיום של טרנזקציה בבלוקצ'יין.
   4. 30 עסקאות בין הצמתים מוגדרות ב Mem-Pool (נרשמות בקובץ לקריאה באיתחול פעם אחת -קובץ JSON) .
   5. קוד בניית בלוקציין. הנחות לקוחות מתוך 1559 EIP:
      1. לכל הארנקים יש 100 מטבעות שנכרו בעבר.
      2. כל בלוק מכיל 4 עיסקאות (כולל עיסקת הכריה) וגודלו אחיד (מבחינת כמות העיסקאות, ולא משתנה.
      3. תגמול כרית בלוק 20 מטבעות לכורה.
      4. עמלת הבסיס שנשרפת (Burn), 1 \* מספר הבלוק שאליו נקשרים (לדוגמה בלוק 3 כל עיסקה מחוייבת ב 2 מטבעות – מקסימום 5 מטבעות).
      5. תגמול לכורה מטבע 1 בגין עדיפות הכנסת העיסקה לבלוק, תוספת לעיסקה מצד המעביר (הכתובת שמשם המטבע מועבר ויורד מהסכום בארנק) . להכניס גם פונקצית בדיקה אצל המעביר שאכן יש לו את הסכום להעברה בארנק.
   6. קוד שריפת המטבעות.
   7. מימוש Segwit (רק הוצאת החתימה מהבלוק -הנח שכל העיסקאות חתומות)
   8. הדפסת תוצרת המאזן של כל ארנק, ופרמטרים סופיים :
      1. סה"כ מטבעות ברשת
      2. סה"כ המטבעות שנכרו בבלוקים של הרשת.
      3. סה"כ המטבעות שנשרפו**.**

בהצלחה מיכה

ההגשה למודל שלושה שבועות, 10 נקודות מהציון הסופי (נ.ב – בדרך תוגש עבודה לטווח שבוע בלבד, לכן לא לבנות על הדקה ה90 ).  
איחור של מעבר לתאריך המקורי 5 נקודות מהציון הסופי.