פרויקט מסכם

סטודנטים יקרים,

- מסמך זה מכיל את הדרישות לפרויקט המסכם.
- הפרויקט כולל שני חלקים: שאלות תיאורטיות וקוד למימוש. קראו בעיון את ההנחיות עבור כל חלק.
- יש לבצע את הפרויקט בשלשות או רביעיות, לא תאושר הגשה ביחידים.
- **כל** סטודנט/ית יעלו קובץ txt בלבד לתיבת ההגשה האישית במודל.
- הקובץ יכיל הכולל קישור לתיקייה משותפת לבחירתם (Google Drivr/OneDrive/GitHub) עם קובץ pdf שכולל תשובות ממוספרות עבור החלק הראשון וקוד המקור עבור החלק השני.
- שם הקובץ יכיל את שם הסטודנט/ית המגישים ולאחר מכן ת.ז של השותפים מופרדים באמצעות פסיקים.
- תאריך אחרון להגשה: **22.8.22.**
- בחלק השני, אני מאפשר לכם לקבוע את ה-API ברכיבים החדשים שתוסיפו (בפרט חתימות מתודות, שמות ממשקים/מחלקות חדשות).
- יש לתעד את הקוד באנגלית בלבד באופן תמציתי כולל פרמטרים.

חלק א' – שאלות תיאורטיות (60 נקודות)

- אורך התשובה יהיה **עד** 5 שורות.
- יש לכתוב את התשובות בעברית בלבד.

1. הסבירו את המונח מטבע דיגיטלי
2. במה שונה כסף דיגיטלי מכסף אלקטרוני?
3. כתבו איזו מהאפשרויות a-d מתארת את המתרחש ברשת ה-bitcoin באופן המדויק ביותר:
   a. Miners מבצעים וולידציה על אוסף pending transactions אותם הם מוסיפים לבלוק. במידה ו-transactions תקינות, הראשון זוכה להוסיף את הבלוק החדש לשרשרת.
   b. Miners מבצעים בנוסף לוולידציה מסעיף a גם ולידציה שכל הבלוקים הקודמים לו אינם כוללים transactions לא תקינות ולכל מטבע יש היסטוריה של transactions תקינות
   c. וולידציה על הבלוקים נעשית על-ידי המשתתפים ברשת
   d. אף אחת מהאפשרויות לא נכונה.
4. הסבירו איזו בעיה נוצרת כאשר מעוניינים לבצע עסקה של תשלום דיגיטלי ללא גורם מתווך מהימן? מהו המונח באנגלית?
5. מיהו הגורם שהוגדר ב-bitcoin protocol לוודא מידע על טרנסאקציה שכמות מסוימת הועברה מחשבון השולח לחשבון היעד ואליו בלבד?
6. מהי המוטיבציה של הגורם המתואר בסעיף 4 לבצע את הווידוא?
7. כתבו איזו מהאפשרויות a-d מתארת את המתרחש ברשת ה-bitcoin באופן המדויק ביותר:
   a. כמות המטבעות המונפקים ברשת ה-bitcoin הינה בלתי-מוגבלת
   b. כמות המטבעות המונפקים ברשת ה-bitcoin הינה מוגבלת ומרגע הנפקת המטבע הראשון, התגמול עבור צירוף block בודד על-ידי miner לא השתנה.
   c. miner אשר באופן תיאורטי פותר ראשון את החידה המתמטית של block ריק לא יוכל לצרף אותו ל-ledger.
   d. כמות מטבעות ה-bitcoin לא יהא גבוה מ-21M
8. כיצד משתמש/ת ברשת ה-bitcoin יכולים לגשת לשרשרת הבלוקים ולבצע פעולות בסיסיות כגון בדיקת יתרה של tokens/בקשה לעדכון ברשת על פעולה אחרת שמעוניינים לבצע?
9. פרטו אלו מפתחות נחוצים למשתמש/ת ברשת ה-bitcoin על מנת להעביר סכום X למשתמש/ת אחר/ה?
10. הסבר/י את המונח פסבדו-אנונימיות

חלק ב' – מימוש קוד (40 נקודות)

1. עליכם להרחיב את פרויקט ה-advanced ledger אשר כלל בין היתר את המחלקות הבאות:
   - Message
   - Block
   - TransactionException
2. בדומה למחלקות שמימשנו, המחלקות החדשות צריכות להיות ממומשות כ-dataclass
3. עליכם להוסיף מתודות ושדות למחלקות קיימות/חדשות ככל הנדרש, על-מנת לאפשר את הפונקציונאליות להלן.

המחלקה Block

1. עליכם להוסיף מתודה אשר עושה וולידציה ל-block בהתאם ללוגיקה אשר תועבר באמצעות פוינטר למתודה או ביטויי למבדה

המחלקה BlockChain

2. מתודה זו מוסיפה הטרנסאקציות זמניות ל-block חדש. אל תשכחו להעביר תגמול ל-miner.
3. add_transaction_to_queue – מתודה זו תקבל אובייקט מסוג Transaction, תבצע וולידציה על הטרנסאקציה וכן בדיקה שאכן ניתן להעביר כמות tokens מחשבון השולח לחשבון המקבל. במידה וכן, הטרנסאקציה תתווסף לתור זמני עד ש-miner יבצע כרייה של הבלוק הבא בשרשרת