שאלות:

1. א. קראו על peer to peer. ??????

ב. לפי מה שלמדנו, תקשורת ביטקוין עובדת בpeer to peer ואין צד שרת או צד לקוח, אך כל העסקאות שאינן מאושרות עדיין מאוחסנות ב"זכרון מאגר", משם הכורים לוקחים עסקאות לאישור. היכן נמצא "זכרון המאגר"?

1. א. למה נועד עץ מרקל? מדוע גיבוב של פרטים הוא אישור מחייב לנכונות שלהם?
2. מהו החיסרון בשימוש בעץ? למה היה עדיף להשתמש בעץ ולא במערך למשל? תן דוגמה בה שימוש במערך היה מניב תוצאה מהירה יותר מעץ ודוגמה הפוכה בה עץ מהיר יותר.
3. קבוצת הכורים BTC.com מחזיקה ב16.9% מכלל הכריות. מישהו הציע לקבוצה לפתוח אפליקציית ארנק שתשלח ישירות אליה את כל העסקאות המתבצעות מהאפליקציה.
4. מדוע אין אפשרות לבצע רעיון כזה?
5. מדוע הקבוצה לא תרוויח מרעיון כזה?
6. פתחו שני ארנקי testnet עפ"י ההוראות בסרטון:

<https://www.youtube.com/watch?v=LfNE29AZ9I0>

בצעו העברה מארנק 1 ל2 תוך הסנפה של wireshark – מה התוצאה? מה ציפינו לראות? מדוע זה לא כך?

שלחו פקטת ביטקוין בשפת C לפי ההוראות הבאות:

<https://github.com/jnewbery/bitcoin-wireshark>

מה התוצאה? מה ציפינו לראות?

פתרונות:

1. ב. מערכת הpeer to peer של ביטקוין עובדת בשני מישורים – סוחרים וכורים. על מנת להיחשף לשרשראות הביטקוין הקיימות ועסקאות שאושרו צריך לאתר
2. א. עץ מרקל נועד להבטחת האמינות של מאשר הבלוק והוא כלי כדי לאמת שעסקה כלשהי שמופיעה בבלוק היא אמיתית ומאושרת. אם העסקה שביצעתי מופיעה בבלוק מסוים, אוכל לראות אם הגיבוב הכללי של העץ תואם לגיבוב של העסקה בO(log n) צעדים (כל פעם בדיקה של גיבוב צומת האב) עד לשורש עץ מרקל. במקרה של מערך, כל בדיקה היתה לוקחת O(n). החיסרון הוא ביצירת הHash של כל העץ במקום הHash של העסקאות בלבד.

Hash merkle – האם הגיבובים שמורים?

<https://en.wikipedia.org/wiki/Merkle_tree>

<https://bitcoin.stackexchange.com/questions/75172/merkle-root-vs-transaction-hashes>

1. א. כל 10 דקות המשימה הגלובלית משתנה (נוסף בלוק) ולכן לא נחסכת עבודה (בדומה לאדם שיעשה 3000 עסקאות עם ארנקים של עצמו וירצה להוסיף את הבלוק לשרשרת – הוכחת העבודה עדיין קיימת. (לא שווה לעשות את זה)

ב. עסקאות מאושרות מפורסמות לכולם, אחרת הן לא נוספות לשרשרת הבלוקים הראשית לכן אין יכולת "להסתיר" עסקאות או לשמור אותם לעצמך.