שאלות:

1. א. קראו על peer to peer. ?????? נדרש המשך לשאלה...

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. בנה עץ מרקל בגובה 3 (בעל 8 מסמכים – תוכן כל מסמך הוא מספר רנדומלי (שונה) בעל 4 ספרות). הנח שפונקציית הHash היא סכום הספרות.

מה שורש העץ?

איזה hash צריך בשביל לאמת את מסמך מספר 3?

1. השלם את עץ מרקל הבא בהנחה שפונקציית הHash היא סכום הספרות ובהנחה שHash שורש העץ הוא: 9.

9

14

8

9



1. קבוצת הכורים BTC.com מחזיקה ב16.9% מכלל הכריות. מישהו הציע לקבוצה לפתוח אפליקציית ארנק שתשלח ישירות אליה את כל העסקאות המתבצעות מהאפליקציה.
2. מדוע אין אפשרות לבצע רעיון כזה?
3. אם היה אפשר, מדוע הקבוצה לא תרוויח מרעיון כזה?
4. פתחו שני ארנקי testnet עפ"י ההוראות בסרטון:

<https://www.youtube.com/watch?v=LfNE29AZ9I0> (כולל קבלה של testnet מאתר כלשהו)

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

ב. מצאו את העסקה בתוך הבלוק שלה - ????נדרש המשך לשאלה..

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.

מסלול האימות נשמר בחתימת המסמך כדי שהמקבל יוכל לאמת שהמסמך לא שונה והחתימה לא זויפה. המסלול כולל את כל הצמתים שנצטרך להשתמש בהם לצורך גיבוב עד לשורש.

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

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

ב.

7

16

5

9

14

17

6

16

14

14

13

13

8

10

9



1. א. עסקאות מאושרות מפורסמות לכולם, אחרת הן לא נוספות לשרשרת הבלוקים הראשית לכן אין יכולת "להסתיר" עסקאות או לשמור אותם לעצמך.
2. 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. ולכן גם אם עסקה לא תיחשף לכולם, ייקח המון זמן עד שתאושר והארנק יהיה איטי מאוד ולא אמין.
3. פרוטוקול TCP לאתר
4. א. ציפינו לראות את פרטי העברת הכספים מארנק אחד לשני בפרוטוקול ביטקוין. בפועל הייתה בקשה לפניה לאתר האפליקציה בפרוטוקול HTTP – והפקטה הייתה מוצפנת.