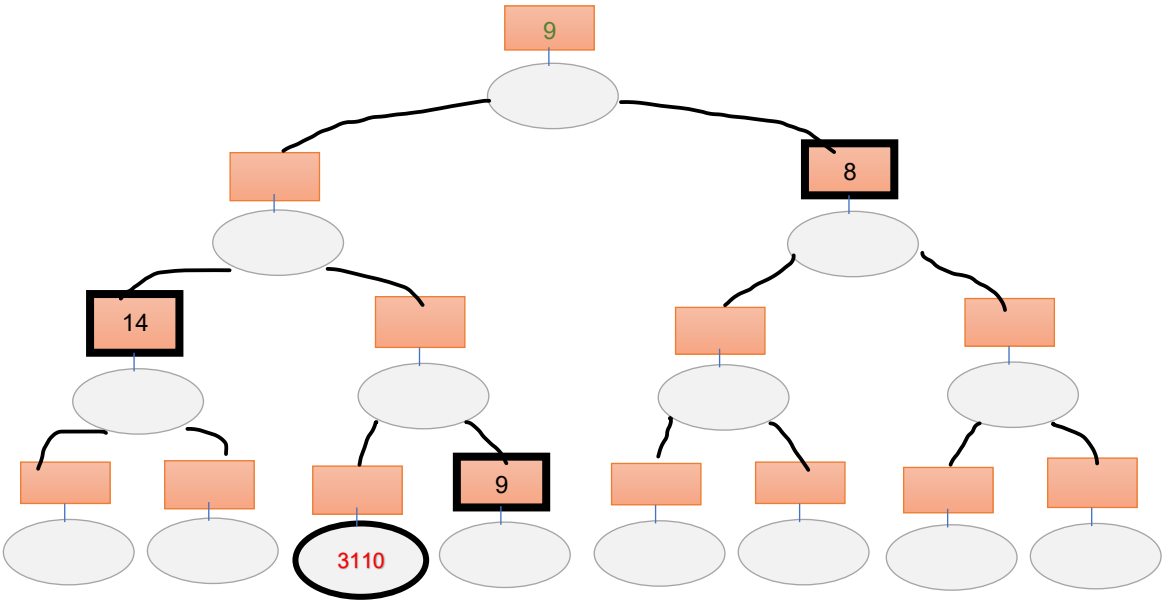
שאלות:

1. א. קראו על peer to peer. מה האינטרס של חברות ציבוריות ושרתים להעביר תעבורת רשת כזו. מדוע שרשת peer to peer לא תתקע? מדוע שרשת הביטקוין לא תתקע?
https://www.isoc.org.il/files/docs/Position_papers_Partiality_Policy_By_ISPs.html.pdf
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"?

2. א. למה נועד עץ מרקל? מדוע גיבוב של פרטים הוא אישור מחייב לנכונות שלהם?
ב. 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.
ג. בנה עץ מרקל בגובה 3 (בעל 8 מסמכים – תוכן כל מסמך הוא מספר רנדומלי (שונה בעל 4 ספרות). הנח שפונקציית Hash היא סכום הספרות.
מה שורש העץ?
איזה hash צריך בשביל לאמת את מסמך מספר 3?
ד. השלם את עץ מרקל הבא בהנחה שפונקציית Hash היא סכום הספרות ובהנחה שHash שורש העץ הוא: 9.



3. קבוצת הכורים BTC.com מחזיקה ב16.9% מכלל הכריות. מישהו הציע לקבוצה לפתוח אפליקציית ארנק שתשלח ישירות אליה את כל העסקאות המתבצעות מהאפליקציה.
א. מדוע אין אפשרות לבצע רעיון כזה?
ב. 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 – אילו נתונים אפשר להסיק מתוך צפייה בעסקה בלבד? מדוע יש הרבה שדות כפולים או שדות שאפשרי להסיק משדות אחרים? לשם מה צריך את כולם?

5. קבוצת כורים מחליטה איזו העברות להוסיף לבלוק שלה לפי גובה העמלה. כיוון שאין הגבלה על גובה העמלה, קבוצות הכורים מוסיפות רק עסקאות בעלי עמלות גבוהות (הקבוצות הגדולות אינן מכניסות עסקאות עם עמלות קטנות במוצהר).
כיוון שישנה תחרות על מקום בבלוק, העמלות הולכות ונהיות גבוהות. באחד מההצעות לפתרון לבעיה, הציעו להגדיל את גודל הבלוק ולהכניס עוד עסקאות. מדוע פתרון זה אינו יעיל?

פתרונות:

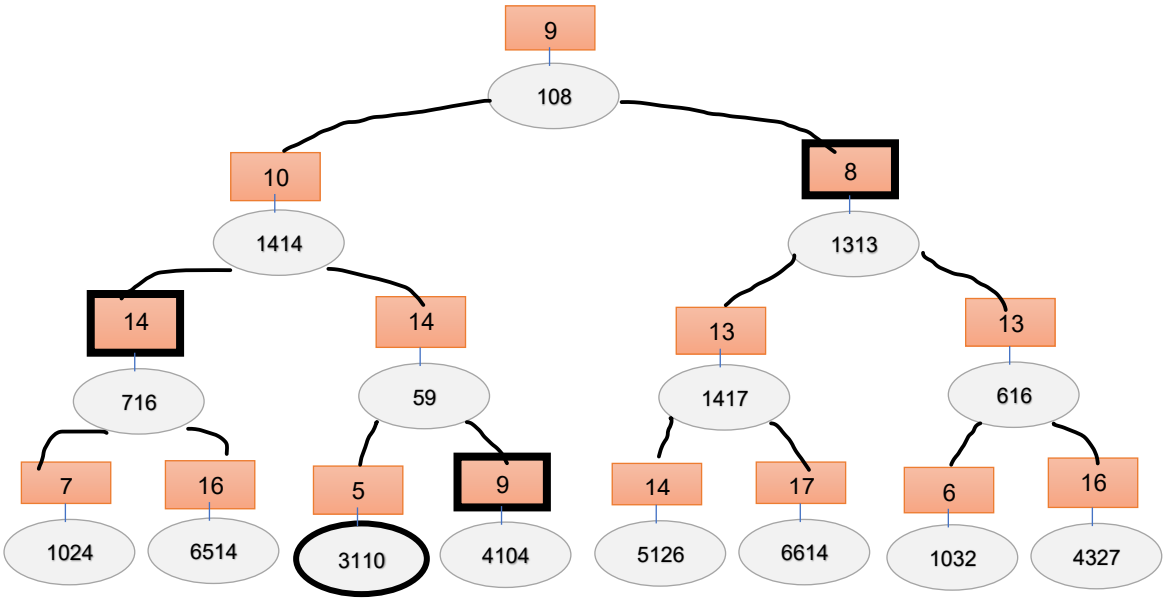
1. א. רשת "עמית לעמית" אכן יכולה להתקע ולא להיות מקודמת ע"י שרתים נפוצים אך לרשת הביטקוין ישנם שרתי DNS הנקראים Seeds שעוזרים לרשת הביטקוין לקבל מענה ולהיות מקודמת ובכך מבטיחים את השארתה של הרשת. אחרת, הרשת היתה איטית ביותר והיתה מצטמצמת לכדי מעגל קטן בלבד.
ב. מערכת הpeer to peer של ביטקוין עובדת בשני 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 ב$O(\log n)$ 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.



3. א. עסקאות מאושרות מפורסמות לכולם, אחרת הן לא נוספות לשרשרת הבלוקים הראשית לכן אין יכולת "להסתיר" עסקאות או לשמור אותם לעצמך.
   ב. 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.
   ג. 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.
   ב. השדות הן שדות שהארנק והאתר מציגים אך לא מועברים ברשת הביטקוין – ראה הרחבה בפרק "העברות"
5. https://blockchaind.net/block-size-increase-not-solution-fees/