שאלות:

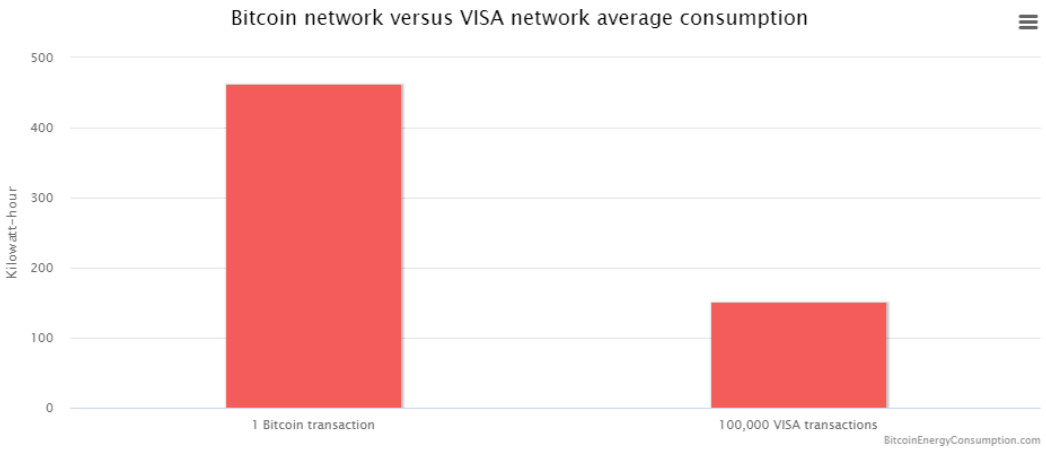
1. קרא על "בעיית הגנרלים הביזנטיים". המצאת הביטקוין הציעה פתרון עבור הבעיה – תאר את הבעיה. היכן אנו נתקלים ב"בעיית הגנרלים הביזנטיים" בהעברת כספים בין קונה ומוכר ביום יום?

   מדוע שימוש בחשבונות בנק לשם העברת כספים פותר בעיה זו? (העברה בנקאית, צ'קים וכו'..) מה החיסרון בפתרון הזה?
   מהו הפתרון החדשני שהביאה המצאת מנגנון הביטקוין?

2. א. קרא על המטבע "Ripple" – מהו השוני המהותי בינו לבין מטבעות קריפטוגרפיים?
   ב. קרא על המטבע "Libra" של פייסבוק. מדוע הוא נחשב יציב יותר מביטקוין?

3. ככל שכוח החישוב גדול יותר, סיכויי הכורים להצלחה גדול יותר ומכאן שכוח החישוב של המחשב שווה כסף. איך אפשר לנצל את העובדה הזו?

4. תהליך הכרייה של הביטקוין הוא בזבזני באנרגיה בצורה חריגה. הנה תרשים המשווה בין בזבוז האנרגיה של עסקה אחת בביטקוין לעומת 100,000 עסקאות בvisa:



   א. תארו פתרון ברשת הביטקוין הפותר את הבעיה בחלוקה שונה של עסקאות לבלוקים.
   ב. מדוע הפיתרון אינו ישים? איזו בעיה נוצרת?

פתרונות:

1. בעיית שני הגנרלים: קבוצת גנרלים שצריכים לתאם התקפה, אך חלק מהגנרלים אינם מהימנים ויש חשש שיזייפו הודעות או שהאויב ישבש הודעות בדרך.
   בכלכלה אנו נדרשים ליצור קונצנזוס על כמות הכסף ובעלות על מטבעות בסחר דיגיטלי (העברות בנקאיות, חשבונות בנק)

   אחת הדרכים לפתור את בעיית הגנרלים הביזנטיים היא על ידי צד שלישי אמין על כולם – ממשלות ובנקים מרכזיים בעסקאות פיננסיות. צד שלישי הוא לא פתרון אמיתי מכיוון שתמיד עומדת האפשרות שהצד השלישי יהפוך ללא אמין מסיבות שונות (מעילה, תקלה או קריסה בגלל התקפה)
   כאשר יותר משני שליש מהמשתתפים הם אמינים בוודאות, ניתנת האפשרות של הצבעה – כך בטוח שתתקבל החלטה של רוב ללא התחשבות ב"מחשבים" הביזנטיים.

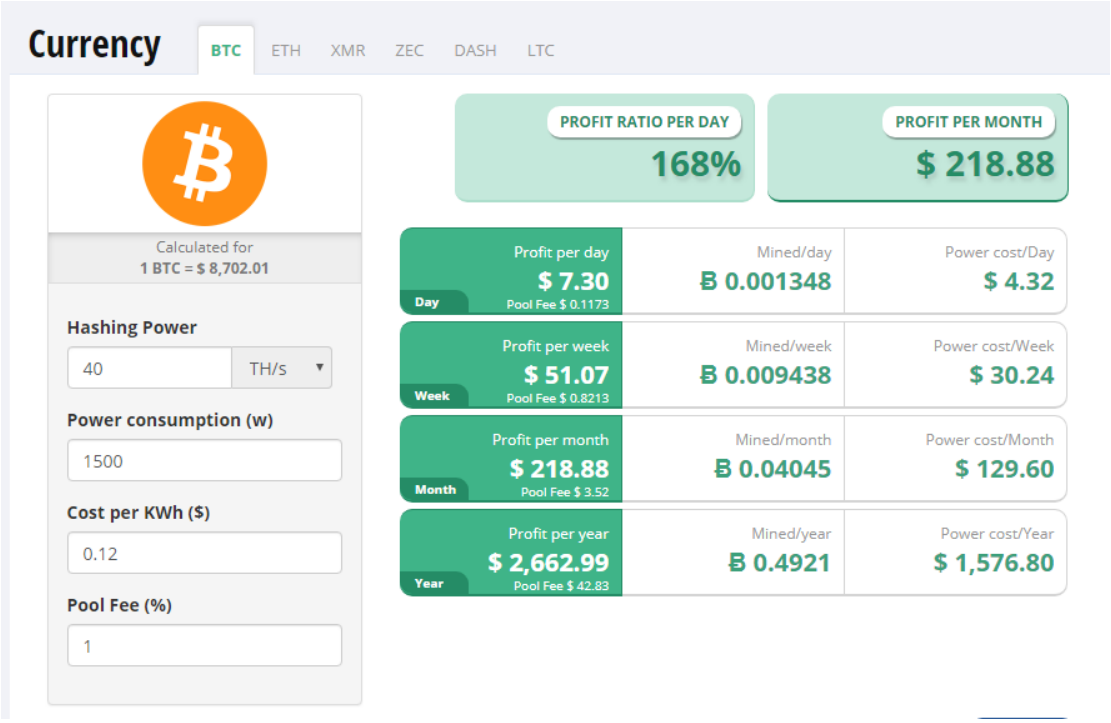
   הפתרון של הביטקוין הוא עקיפת הבעיה ע"י הוכחת עבודה כך שאין זהות לכל משתתף אלא

הוכחת אמינות ולכן, בהקבלה לגנרלים, לגנרלים לא אכפת מי החליט על השעה אלא שהשעה שהופצה היא אמינה. הם יכולים לבדוק ע"י פונקציית Hash שזאת ההחלטה עבורה נדרש קונצנזוס.
הסברים:
https://www.youtube.com/watch?v=A-mNgqJETQg
https://www.youtube.com/watch?v=YJHcoHxfor4
(http://www.forbes.co.il/news/new.aspx?Pn6VQ=E&0r9VQ=EEIGJ)

2. א. Ripple הוא מטבע פיאט (כלומר ערכו ניתן לו מתוקף חוק או מוסכמות), Bitcoin הוא אינו מטבע פיאט ועצם כרייתו מעניקה לו את שוויו.
https://blockonomi.com/permissioned-vs-permissionless-blockchains/
ב. Libra הוא מטבע שעומדים מאחוריו נכסים בעלי ערך ממשי שאינו תלוי בערך המטבע ולכן שוויים יישאר פחות או יותר קבוע (בתים או קרקעות).

https://bitcoin.stackexchange.com/questions/7609/how-ripple-is-different-from-bitcoin-and-other-crypto-currencies?rq=1

3. אתר שמציע שירותים עבור ניצול כוח החישוב של המחשב ע"י בדיקה זריזה של יכולת הכרייה –
https://www.cryptocompare.com/mining/calculator/btc?HashingPower=40&HashingUnit=TH%2Fs&PowerConsumption=1500&CostPerkWh=0.12&MiningPoolFee=1
(מחשבון רווח עבור יכולת כרייה)



4. א. לכלול בכל בלוק יותר עסקאות – כרגע יש 3000 עסקאות בערך בכל בלוק, צריכת האנרגיה של כל בלוק היא קבועה ולכן היה אפשרי לכלול 300,000 עסקאות בבלוק אחד.
ב. משתי סיבות הפתרון אינו ישים:
   i. גודל הבלוק היה כבד מדי בשביל ניוד ברשת ובשביל שליחה ואישור (גם ככה גודל הבלוק העכשווי הוא גבולי ומאסיבי)
   ii. כיוון שייקח יותר זמן לעיבוד ואישור כל כך הרבה עסקאות בכל פעם, קצב הקושי ישתנה ויהיה קשה יותר לאזן את קצב הכרייה לבלוק ב10 דקות בממוצע.