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?

1. קרא על המטבע "Ripple" – מהו השוני המהותי בינו לבין מטבעות קריפטוגרפיים?

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>)

1. 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/>

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