בס"ד

<u>פרויקט מסכם מטבעות קריפטוגרפים</u>

חלק א'

1. מטבע דיגיטלי הוא מטבע וירטואלי ללא ערך פיזי, אך ניתן להשתמש בו על מנת להעביר ערך בצורה דיגיטלית - ברשת האינטרנט (כמו תשלום). מטבעות וירטואליים מתחלקים ל3 קטגוריות לפי כיווני זרימת חליפין של המטבע: רשת סגורה, זרימה חד-כיוונית, המטבעות הדיגיטליים משתייכים לקטגוריה השלישית שהיא זרימה דו-כיוונית - שניתן להמיר מטבעות דיגיטליים למטבעות מדינתיים וכן להפך. ערכם של המטבעות הדיגיטליים נקבע לפי רשת המשתמשים ולא לפי גוף מרכזי אחד.

2. כסף אלקטרוני הוא כנגד ערך כספי פיזי שמאוחסן אצל גורם כלשהו, לעומת זאת כסף דיגיטלי זה כסף שהוא נקוב בסוג של מטבע אחר דיגיטלי.

3. b

4. הבעיה שנוצרת כאשר אנחנו רוצים לבצע עסקה ללא גורם מתווך מהימן היא, שמשתמש יכול להשתמש באותו מטבע יותר מפעם אחת ע"י שיכפול או זיוף של פרטי העסקה. בעיה זו נקראת double spending (הטכנולוגיה של block chain באה לפתור בעיה זו).

5. הגורם הוא miner - על מנת למנוע double spending, הוגדרו בprotocol bitcoin minerים - אלו משתמשים מיוחדים ברשת. כאשר משתמש רגיל רוצה לבצע עסקה, הוא משדר מסר פומבי למשתמשי הminer, המסר מכיל מידע על כמות מסוימת של bitcoin שיועבר מהחשבון שלו לחשבון של אדם אחר - המקבל. הminerים מבצעים את תהליך הווידוא של הטרנזקציה ע"י פתרון בעיה מתמטית ובאמצעות הפתרון נוצר block חדש שמכיל אוסף של טרנזקציות שלא נמצאות בשרשרת ומצרפים אותו לשרשרת.

6. הminer שמבצע את הווידוא, (הראשון שפותר את החידה המתמטית ומוסיף את הblock החדש לblockchain) מקבל עמלות ומטבעות חדשים שמונפקים.

7. d

8. על מנת שמשתמש ברשת הbitcoin יוכל לבצע כל מיני פעולות ושימוש במטבעות הbitcoin, עליו להשתמש באפליקציה או תוכנה או שירות אחר של ארנק דיגיטלי - wallet. המטבעות לא מאוחסנים בבעלות המשתמש אלא הwallet מאחסן את המפתח הפרטי של המשתמש ובכך מאפשר למשתמש לגשת לשרשרת הבלוקים, למידע שלהם ולביצוע פעולות שונות שמעוניין לבצע.

9. לכל משתמש ברשת הbitcoin נחוץ מפתח ציבורי ומפתח פרטי. מפתח פרטי הוא חתימה אלקטרונית חד חד-ערכית והמפתח ציבורי הוא כתובת הbitcoin שאליו אנחנו רוצים לשלוח/לקבל (כמו מספר חשבון בנק). לכל מפתח ציבורי יש מפתח פרטי משלו ועל מנת לשלוח סכום מסוים למפתח ציבורי כלשהו(משתמש אחר), יש צורך בחתימה של המפתח הפרטי שמתאים לו.

10. פסבדו-אנונימיות זה אנונימיות חלקית, בעצם ביצוע פעולה כלשהי בצורה פומבית אך חלקה קוראת בצורה אנונימית למשל, על מנת לנהל רשת block chain, יש צורך באנונימיות חלקית, אנחנו רוצים שביצוע טרנזקציה יעשה בצורה פומבית על מנת שנדע שטרנזקציה מסוימת אכן קרתה וניתן יהיה לבצע וולידציה, אך אנחנו רוצים שהזהות של אלו שמבצעים את העסקה (העברה של bitcoin בין שני מפתחות פומביים) ושיוך המפתח הפומבי למפתח הפרטי של אותו אדם יישאר אנונימי.