**תהליך הכרייה**

*כריית* ביטקוין הוא שם הפעולה המתמטית שנעשית כדי לאשר "*בלוק*" מסוים. כאשר אחד מהכורים מצא את ***הפתרון*** לבעיה המתמטית, הוא מצרף את הבלוק שאישר לתוך שרשרת הבלוקים (blockchain) הארוכה ביותר הקיימת (ישנו שורש שרשרת אחד לכל הבלוקים של ביטקוין).

*מציאת פתרון* היא תהליך *חישוב ערך הNONCE* הוא תהליך הכרייה עצמה. הפעולה היא חישוב סזיפי עבור מעבדים ומכונות חישוב ומקבילה לתהליך כריית משאב טבע.

הפעולה היא ניסיון להפוך פונקציה חד כיוונית. SHA256 היא פונקציה המפיקה מספר מהודעה כלשהי m עם תווים שמרכיבים אותה.

מטרת התהליך היא חישוב ביטוי "nonce" שהוספה שלו אל הודעה m והפעלה של הפונקציה SHA256 כך: SHA256(m+x) תיתן מספר כלשהו.

ככל שקיים תנאי מחמיר יותר על התוצאה הנדרשת כך גודלת רמת הקושי כיוון שאין חוקיות לכיוון הזה בפונקציה ויש לבדוק את כל האפשרויות.

SHA256(m+x)<(2^224)/D כך שD היא רמת הקושי. ככל שD גדול יותר, x יהיה קשה יותר לחישוב (כי הפונקציה צריכה להניב מספר קטן יותר).

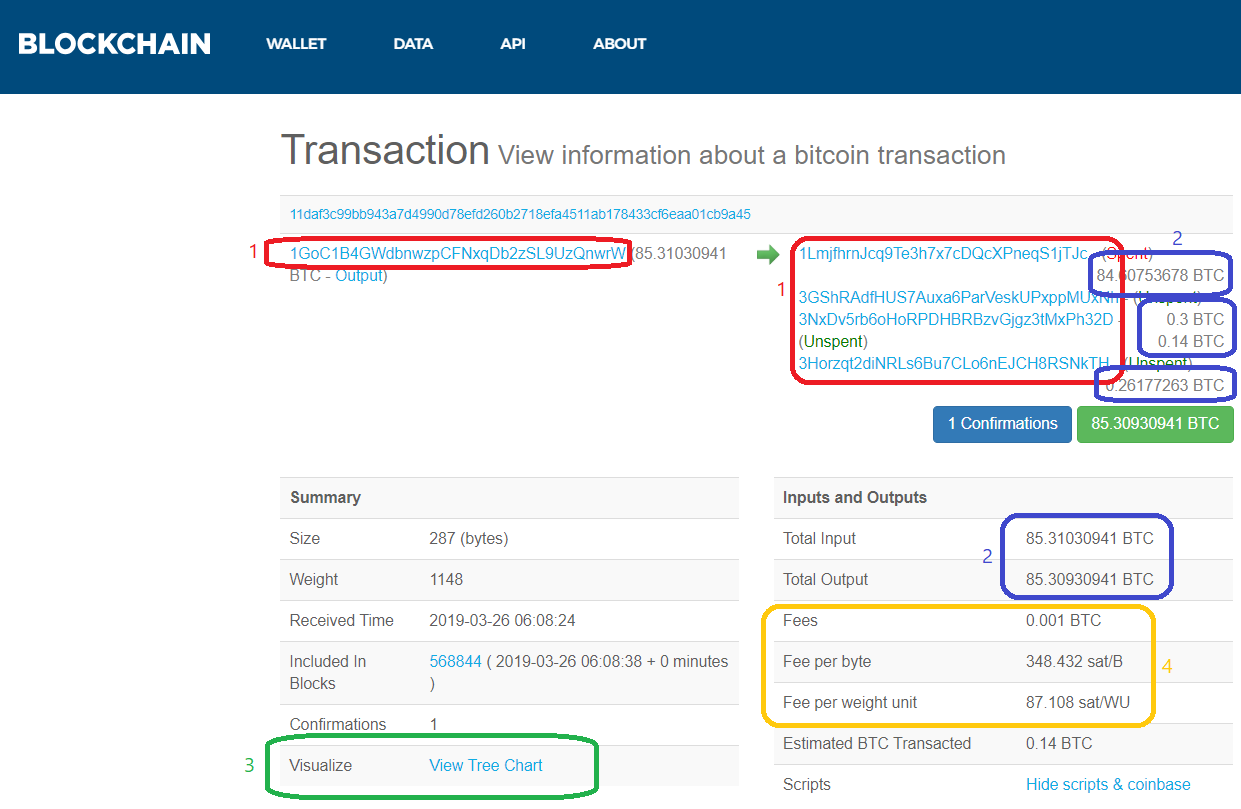
<http://blockchain.mit.edu/block> (חישוב nonce קטן ממספר עם 4 אפסים).

<https://www.youtube.com/watch?time_continue=542&v=_160oMzblY8>

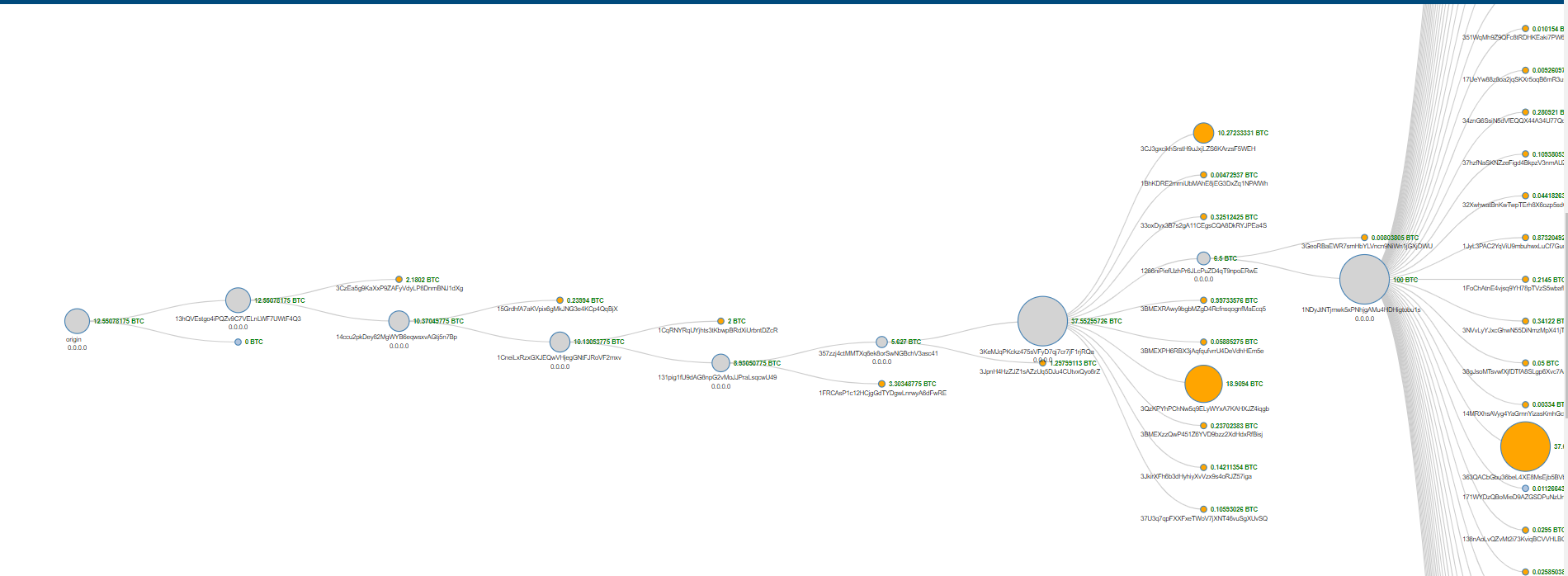
<http://blockchain.mit.edu/blockchain>

***עסקה*** (Transection) היא מבנה שמכיל 4 שדות עיקריים:

1. מפתחות ציבוריים של השולחים והמקבלים (במקרה של יצירת מטבע חדש אין מפתחות שולחים)
2. סכום הכסף שנשלח – מען ונמען
3. קישור לעסקאות קודמות של המטבעות משלב יצירתן
4. עמלה – סכום שיקבל מי שאישר את ההעברה.
5. Hash – משוכלל של כל פרטי העסקה.

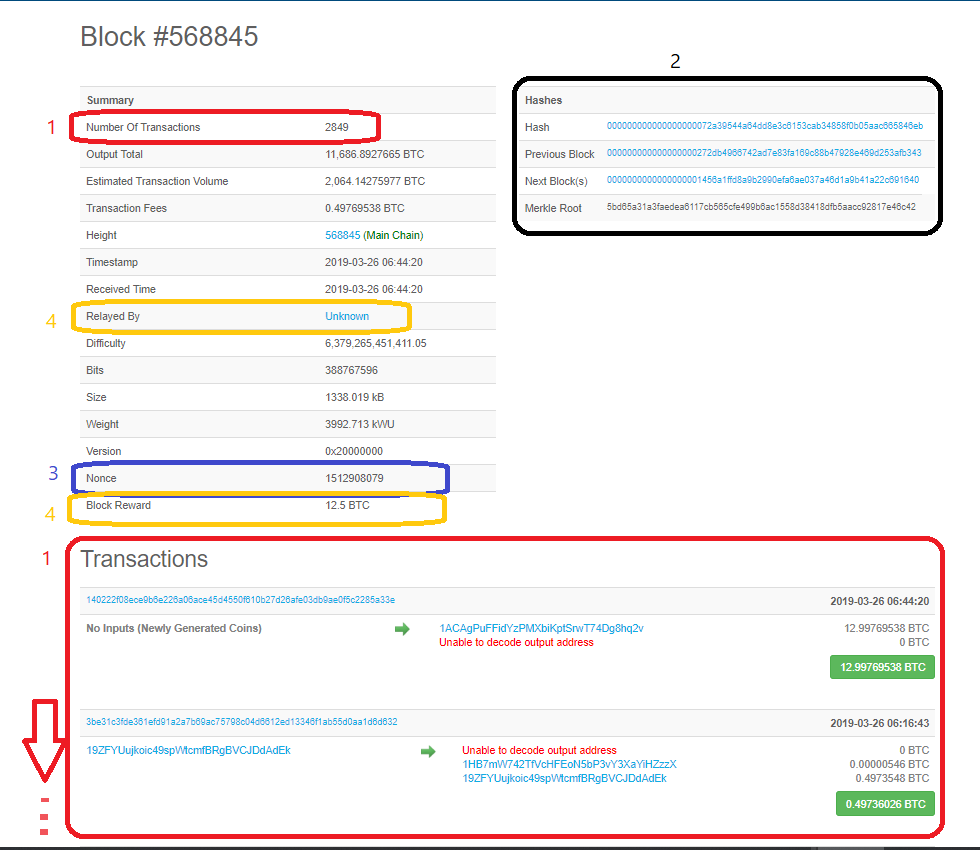
**

דוגמא להתפשטות של כסף משלב יצירת המטבע



***בלוק*** הוא מבנה שמכיל:

1. כ3,000 עסקאות
2. Hash: של הבלוק הקודם, הבלוק הבא (אם קיים) ובלוק השורש של *עץ המרקל* (אישור כל העסקאות בבלוק)
3. *פתרון החידה* של הבלוק (nonce)
4. סכום הרווח של כורה הבלוק (מוצא פתרון הnonce).



<https://www.blockchain.com/btc/block/00000000000000000011f05cfcd35aa8ae5d7bf8f6673e7a86089839bab40948>

כורה הבלוק הנוכחי הוא זה שמחליט האם להכניס עסקה מסוימת לתוך הבלוק שאותו הוא עומד לאשר. הוא מחליט על פי "עמלת האישור" שנקבעת ע"י המשלם.

ככל שהעמלה גבוהה יותר, יש אינטרס גבוה יותר לכורים להוסיף את העסקה לבלוק שלהם ולכן העסקה מאושרת מהר יותר ולכן גם מאובטחת יותר לטווח הקצר.

