**תהליך הכרייה**

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

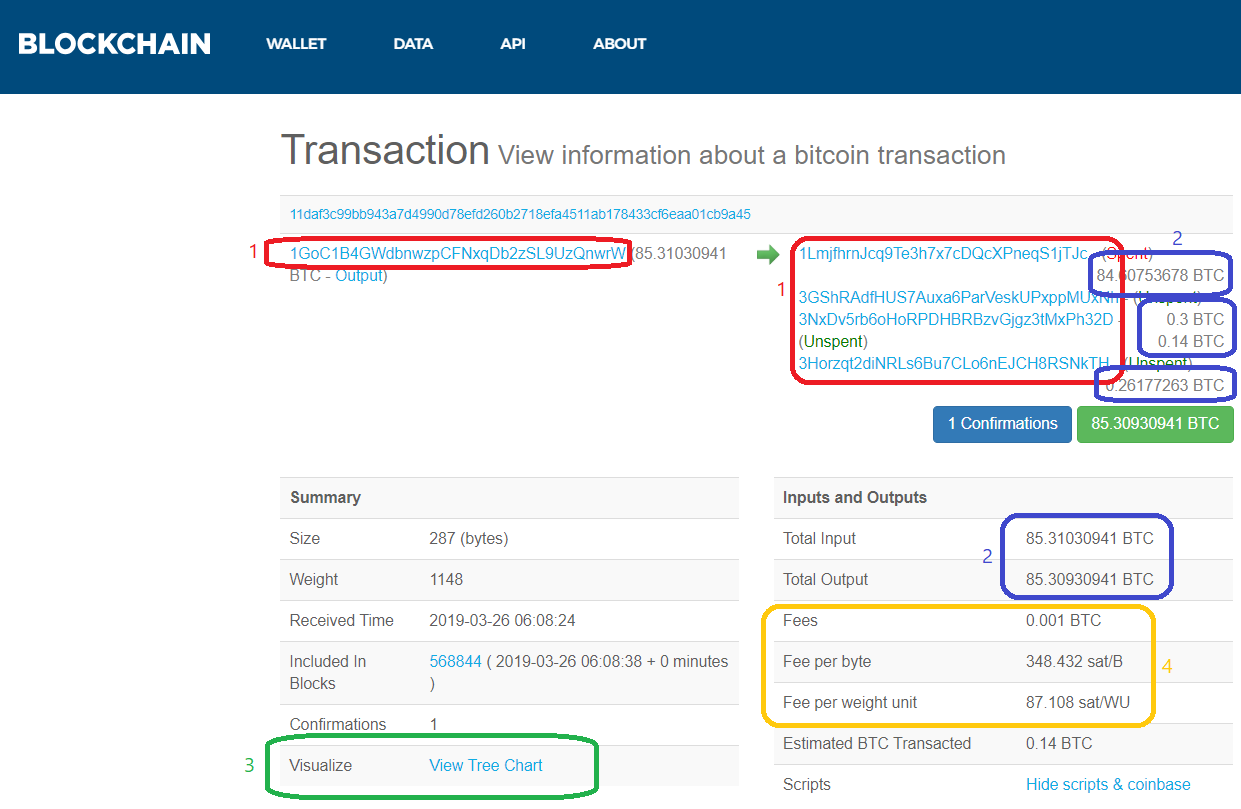
**עקרון המערכת**

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

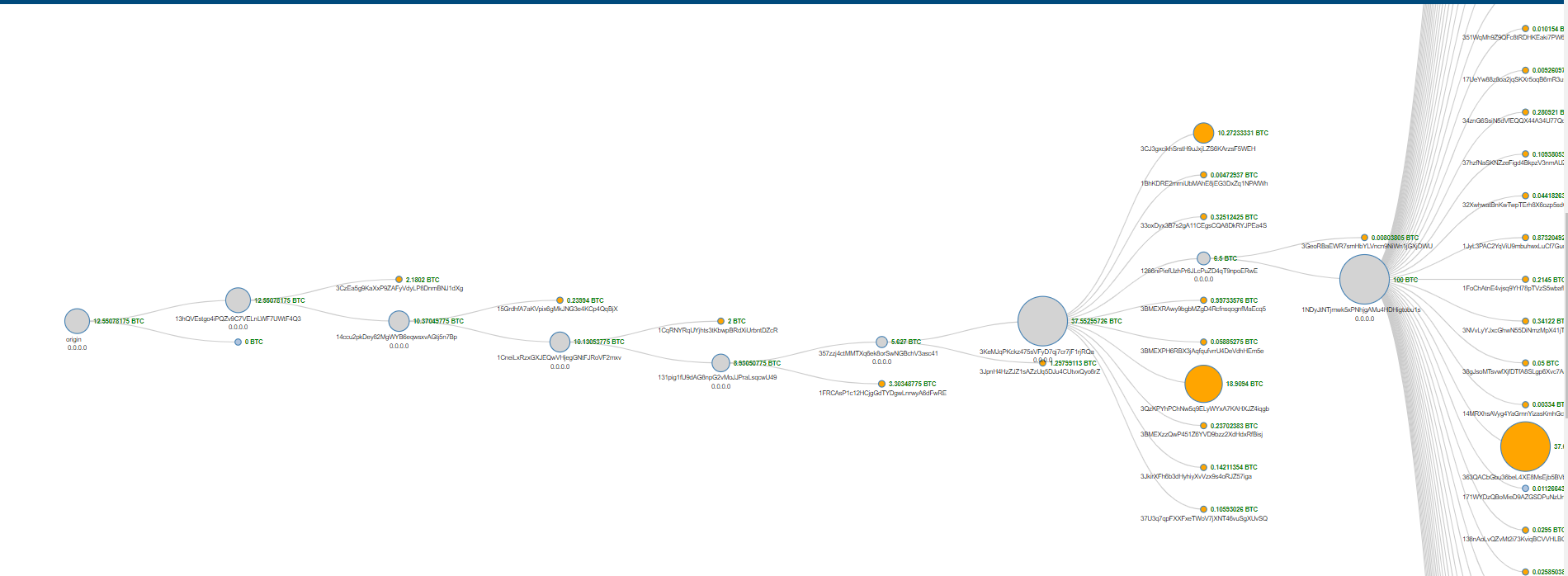
<http://blockchain.mit.edu/blockchain>

***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.

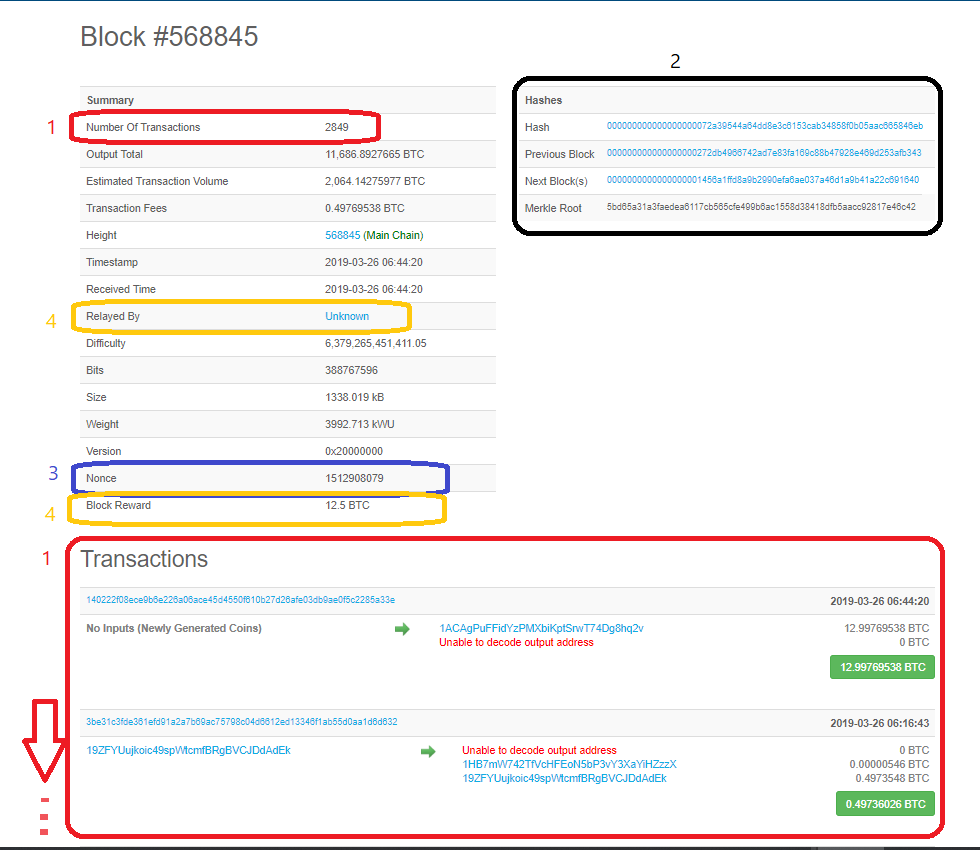
**

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) **והשם שלו?**



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

*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).

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.

