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).

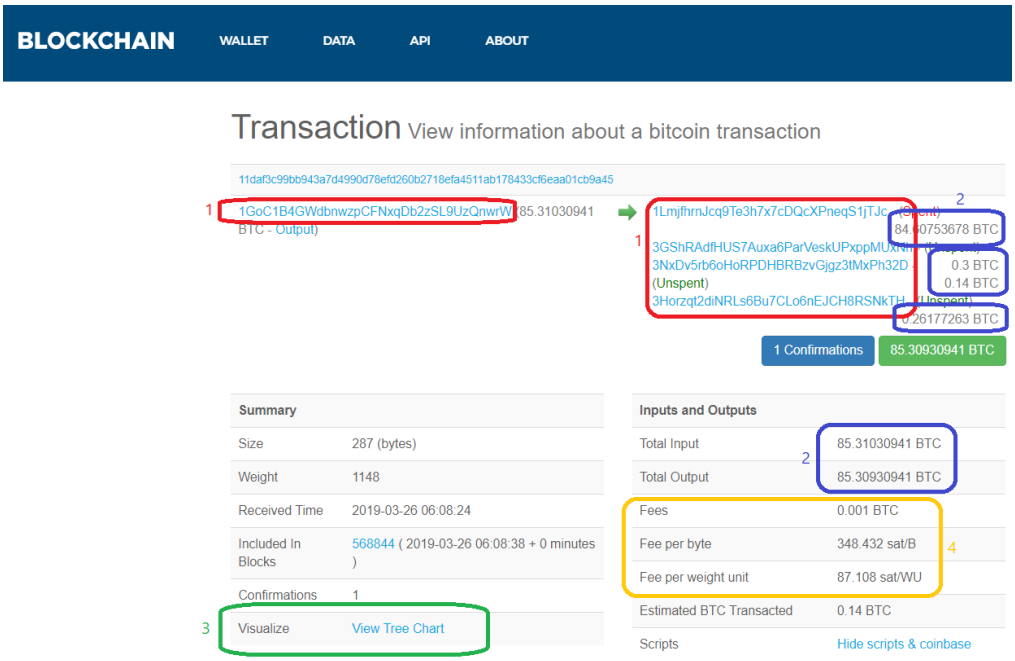
http://blockchain.mit.edu/block (חישוב nonce קטן ממספר עם 4 אפסים).

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

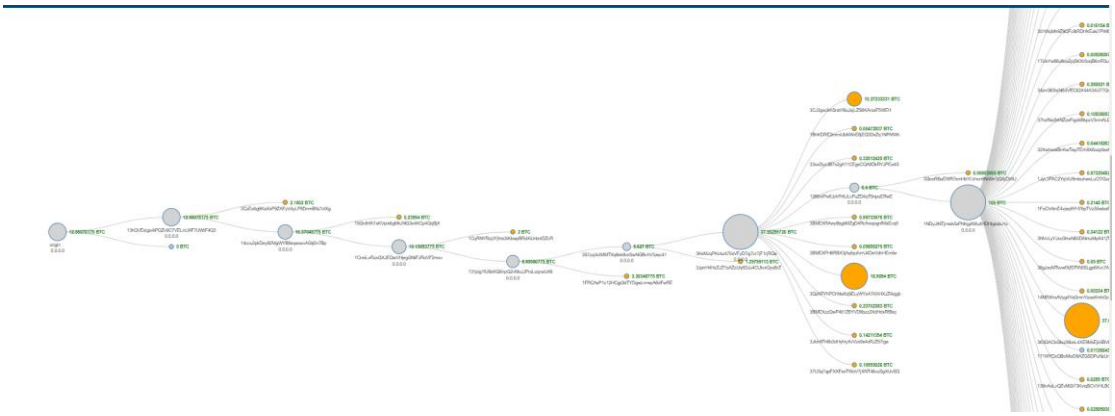
http://blockchain.mit.edu/blockchain

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.

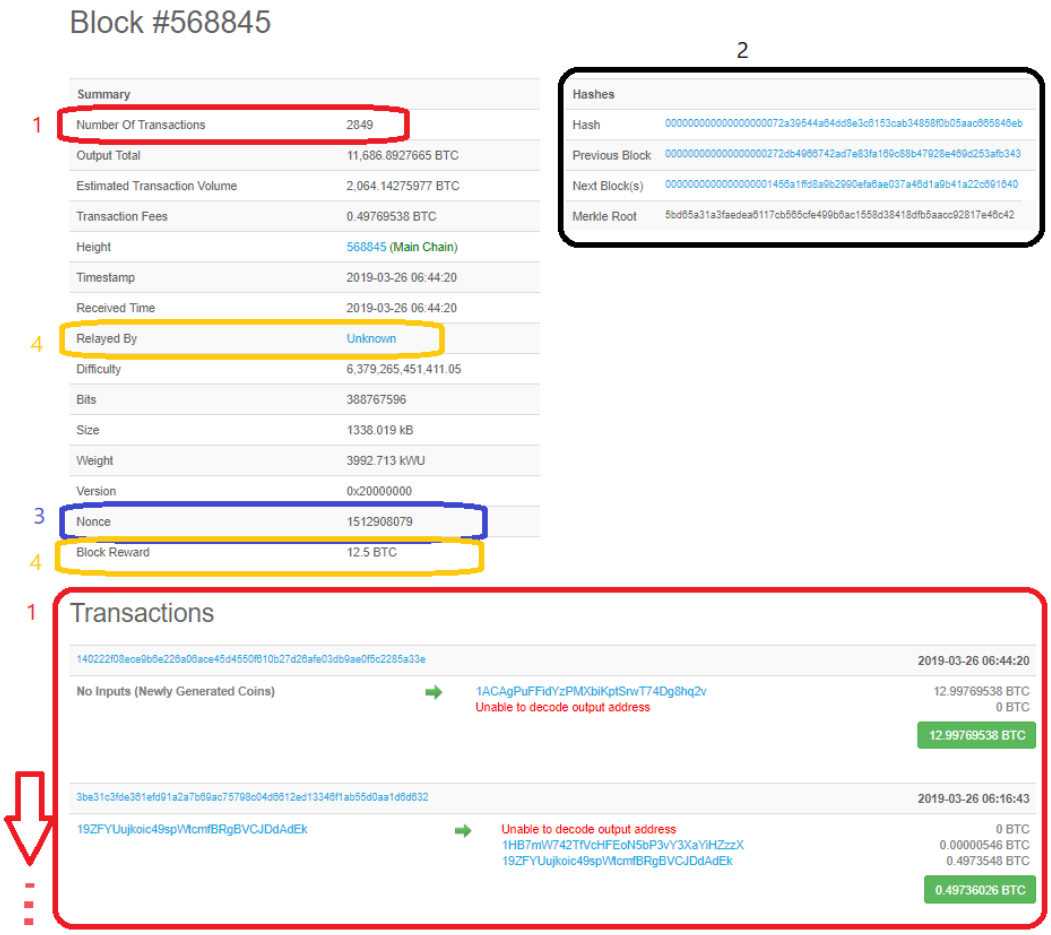


דוגמא להתפשטות של כסף משלב יצירת המטבע



בלוק הוא מבנה שמכיל:

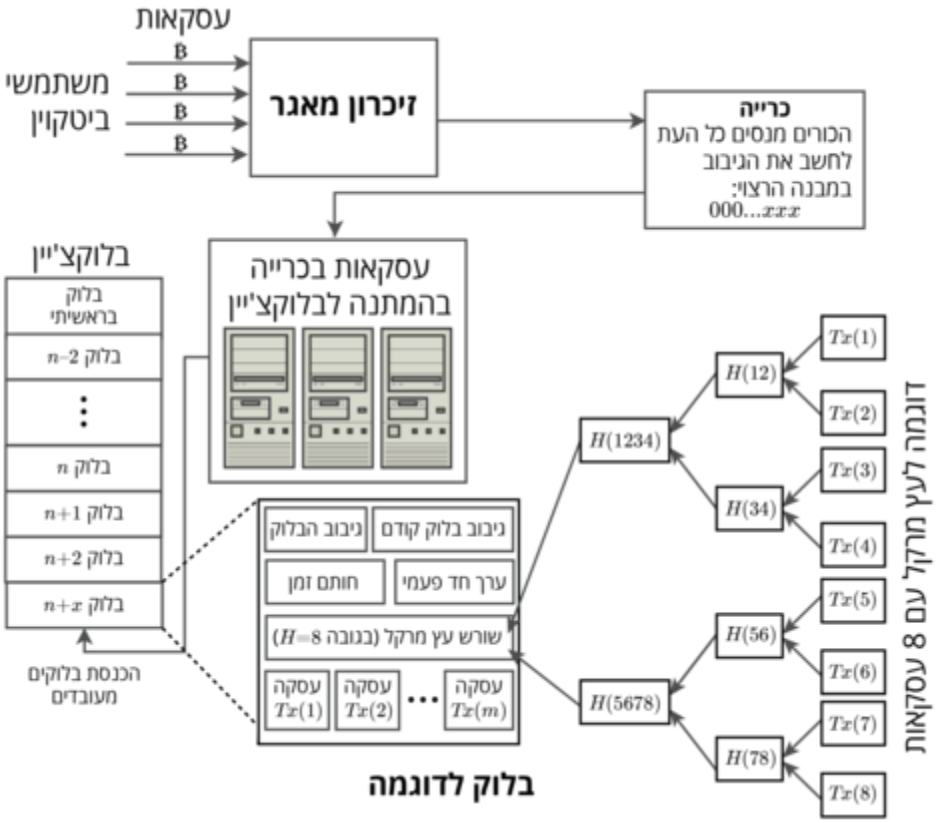
1. כ3,000 עסקאות
2. Hash: של הבלוק הקודם, הבלוק הבא (אם קיים) ובלוק השורש של *עץ המרקל* (אישור כל העסקאות בבלוק)
3. *פתרון החידה* של הבלוק (nonce)
4. סכום הרווח של כורה הבלוק (מוצא פתרון הnonce).



https://www.blockchain.com/btc/block/0000000000000000000011f05cfcd35aa8ae5d7bf8f6673e7a86089839bab40948

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.



ברגע שבלוק מאושר, כלומר שה"חידה" של הבלוק נפתרה, נוסף הבלוק אל "שרשרת הבלוקים" (Blockchain). כיוון ש שרשרת הבלוקים היא רשימה מקושרת בבלוק מצוין איזה בלוק הוא הקודם (כלומר האחרון). במידה ו"נפתרים" מספר בלוקים במקביל, ישנו פיצול בשרשרת.

השרשרת הקובעת היא השרשרת הארוכה ביותר. ברגע שאחת מהשרשרות היא הגדולה, נפסלת השרשרת השנייה וכל העסקאות בה מתבטלות.

לכן, על מנת להבטיח אישור עסקה החלטי בביטקוין, טוב לחכות מספר אישורים של בלוקים כדי להיות בטוח שהעסקה שאושרה לא תתבטל.

"חידת הבלוק" קשה בצורה מספקת כדי להבטיח קצב אחיד של פתרון אחידה בממוצע של 10 דקות לבלוק. כאשר קצב הפתרון עולה (מכל מיני סיבות – יותר משקיעים, אמצעים מתקדמים יותר) החידה נעשית קשה יותר (נוסף עוד 0 כדרישה לפתרון) ושוב זמן פתרון ממוצע חוזר ל10 דקות לבלוק.

איך נוכל לדעת בוודאות שהמידע על גבי הבלוקצ'יין הוא אכן מידע מהימן? מה מונע ממשתמשים עם כוונות זדוניות לחדור לנתוני הבלוקצ'יין ולחבל בנתונים לטובתם האישית?

כאן בדיוק נכנס תפקידם של הכורים. כאשר בלוק עסקאות נוצר, הכורים לוקחים את הבלוק ומעבירים אותו תהליך מתמטי מסוים (מיד נרחיב) אשר בסופו הבלוק הופך למשהו אחר. הכורים משלבים את המידע המצוי בבלוק עם נוסחאות מתמטיות ויוצרים מהכמות האדירה של המידע שנמצא בבלוק רצף

ייחודי וקצר יחסית של תווים המורכב משילוב של אותיות ומספרים. בסיום התהליך, רצף התווים הייחודי נשמר על גבי הבלוק. ליתר דיוק, בסופו של הבלוק.

התהליך הזה ידוע כגיבוב או באנגלית, Hashing. ל Hashing יש כמה תכונות מעניינות. הראשונה היא שקל מאוד להפיק מאוסף של מידע את ה Hash שלו, אך כמעט בלתי אפשרי לחלץ מרצף תווי ה Hash את המידע בחזרה. תכונה נוספת וחשובה של Hashing היא שיצירה של Hash ספציפי על אוסף נתונים תמיד תניב את אותה תוצאה, אך שינוי אפילו של תו אחד בודד במידע המקורי, יגרום ליצירת Hash שונה לחלוטין מה Hash הקודם. שתי תכונות אלו הינן קריטיות לתפקוד רשת הביטקוין ומיד נסביר מדוע. אך חסרים לנו עוד כמה פרטים לסיום תיאור התהליך. בכדי לייצר Hash לבלוקי עסקאות, הכורים לא משתמשים רק במידע של העיסקאות שבוצעו בבלוק אלא גם בפיסת מידע נוספת וחשובה. פיסת מידע זו היא ה Hash של הבלוק הקודם. מכיוון שכך, וה- Hash של בלוק קיים מבוסס על ה- Hash של הבלוק הקודם, אנו מקבלים מצב שבו נוצרת מעיין חתימת שעווה דיגיטלית ייחודית לכל בלוק. חתימה זו מאשרת, שבלוק זה וכל הבלוקים הקשורים אליו, הינם בלוקים חוקיים ואמיתיים והנתונים השמורים בהם הינם מהימנים.

הסיבה היא, שמכיוון ואם מישהו ינסה לחבל בנתוני בלוק עסקאות, הדבר יגרום מיידית לשינוי ה Hash שאותו בלוק יפיק וכל הבלוקים שיופיעו אחריו וכל המשתמשים ברשת הביטקוין ידעו על כך ויזהו את הזיוף.

כריית ביטקוין זוהי בעצם הצורה שבה כורי הביטקוין סוגרים ומאבטחים כל בלוק על גבי הבלוקצ'יין. אבל הם לא עושים את זה בחינם. בכל פעם שכורה מייצר בהצלחה Hash לבלוק הוא מקבל בתמורה 12 וחצי בערך מטבעות ביטקוין שנוספים למחזור המטבעות הקיים ומוענקים לו כפרס על עבודת החישוב הקשה שביצע. הבעיה היחידה בתגמול הכורים בצורה הזאת היא שמאוד קל לייצר Hash לבלוק מסוים. אם הכורים יתבקשו רק לייצר Hash לעסקאות, כל 21 מיליון מטבעות הביטקוין האפשריים ייכרו בתוך כמה דקות בלבד. כדי להתמודד עם המגבלה הנ"ל הפתרון המתבקש הוא פשוט: צריך להפוך את התהליך לקשה יותר.

פרוטוקול הביטקוין מבצע זאת על ידי יצירת תהליך נוסף שנקרא "**Proof of work**".

Proof of work כמו ששמו מרמז, קיים במטרה לגרום לכורים להוכיח שהם עבדו – וקשה. Proof of work אומר שרשת הביטקוין לא מבקשת מהכורים לייצר סתם עוד Hash רגיל לבלוק העסקאות, אלא דורשת מהם שה- Hash יראה בצורה מסוימת שבה יש בתחילתו של כל Hash מספר מסוים של אפסים. זה לא קל, כי כשמייצרים Hash על קובץ מידע, אין שום דרך לחזות איך ה Hash יראה לפני שמייצרים אותו ובכל פעם שמשנים אפילו נתון קטן בקובץ המידע, ה Hash נראה אחרת לגמרי.

הכורים לא אמורים כמובן לשנות את נתוני העסקאות על גבי הבלוק אך הם כן יכולים וצריכים לשנות את המידע שאותו הם מצמידים לבלוק על מנת לחשב את ה Hash שלו בפורמט הנדרש.

פיסת המידע הרנדומלית הזאת שמתווספת לנתוני העסקאות בבלוק נקראת Nonce והיא משמשת את הכורים בייצור ה Hash של הבלוק. אם ה Hash שחושב אינו מתאים לפורמט הרצוי, ה Nonce משתנה (בצורה רנדומלית) וכל התהליך מבוצע שוב מההתחלה. כפי שכבר ניחשתם, יכול לקחת מספר רב של נסיונות עד שמתקבל פורמט ה Hash הרצוי. ככל שכח המחשוב של הכורה גדול יותר כך גם הסיכויים שיצליח לייצר ראשון את ה Hash שדורש אלגוריתם הביטקוין. פרוטוקול הביטקוין לקח בחשבון שעם הזמן מחשבים עוצמתיים ייכנסו לזירת הכרייה והגיע מצויד במנגנון משוכלל להתאמת רמת הקושי ברשת לכוח המחשוב שלה. ככל שכוח המחשוב ברשת גדל וקצב מציאת הבלוקים הולך ועולה, אלגוריתם הביטקוין מעלה באופן אוטומטי את רמת הקושי במציאתם ואישור בלוקי עסקאות ומבטיח בכך לשמור על שיווי משקל ברשת והפצה איטית ומדודה של המטבעות החדשים. זו היא הסיבה שכורי הביטקוין כל הזמן פועלים במרוץ חימוש אגרסיבי על מנת להשיג חומרה חזקה ומהירה יותר כדי לבצע את מלאכת הכרייה ולזכות בביטקוין חדשים כתגמול.

http://www.cryptobit.co.il/cryptobit/%D7%9B%D7%A8%D7%99%D7%99%D7%AA-%D7%91%D7%99%D7%98%D7%A7%D7%95%D7%99%D7%9F/