**מבוא לביטקוין**

הביטקוין הוצג לעולם בשנת 2009 ע"י [Satoshi Nakamoto](https://en.wikipedia.org/wiki/Satoshi_Nakamoto) כתוכנת open source.

הביטקוין הוא למעשה כסף אלקטרוני מבוזר, כלומר ערכו לא נקבע לפי ערך סחורה או לפי קביעה של גוף מרכזי אחד, אלא לפי הסכמה בין רשת המשתמשים.

עסקאות המתבצעות ברשת ה Bitcoin נקראות טרנזקציות והמשמעות היא רישום ב"ספר חשבונות" ציבורי הנקרא BlockChain.

את ה Bitcoin ניתן לשלוח ממשתמש למשתמש על גבי Bitcoin network ללא הצורך במטווח כלשהו.

יצירת מטבעות Bitcoin מתבצעת בתהליך הנקרא כרייה, כל אדם יכול למעשה להפיק Bitcoin - "כריית"

ה Bitcoin היא בעצם "פרס " עבור תחזוקת ה BlockChain- והוספת בלוקים חדשים – היכולת לייצר בלוק חדש אשר ניתן להוספה לChain נקבע על ידי כוח החישוב הקיים ברשת. הפרוטוקול קובע שבממוצע כל 10 דקות יתווסף בלוק חדש ל - BlockChain.

רשת הBitcoin היא רשת מבוזרת, ותוכנת ה Bitcoin מבוססת על פלטפורמת "קוד פתוח" כלומר קוד הניתן לעריכה ושינוי על ידי המפתחים ברשת. נהלי העבודה כגון כללי המסחר וכללים טכנים נוספים ברשת זו נקבעים על ידי קהילת המשתמשים, וכללים אלו ניתנים לשינוי בהינתן רוב מכריע המסכים על שינוי בכללי העבודה.

במהלך חיי מטבע ה Bitcoin הגיעה חלק מהקהילה להחלטה כי יש לשנות את "כללי המשחק", הדבר גורם למחלוקות בקהילת המשתמשים מסיבות מגוונות, ובשל חוסר הסכמה של כלל המשתמשים נוצרים פיצולים (Forks) ברשת.

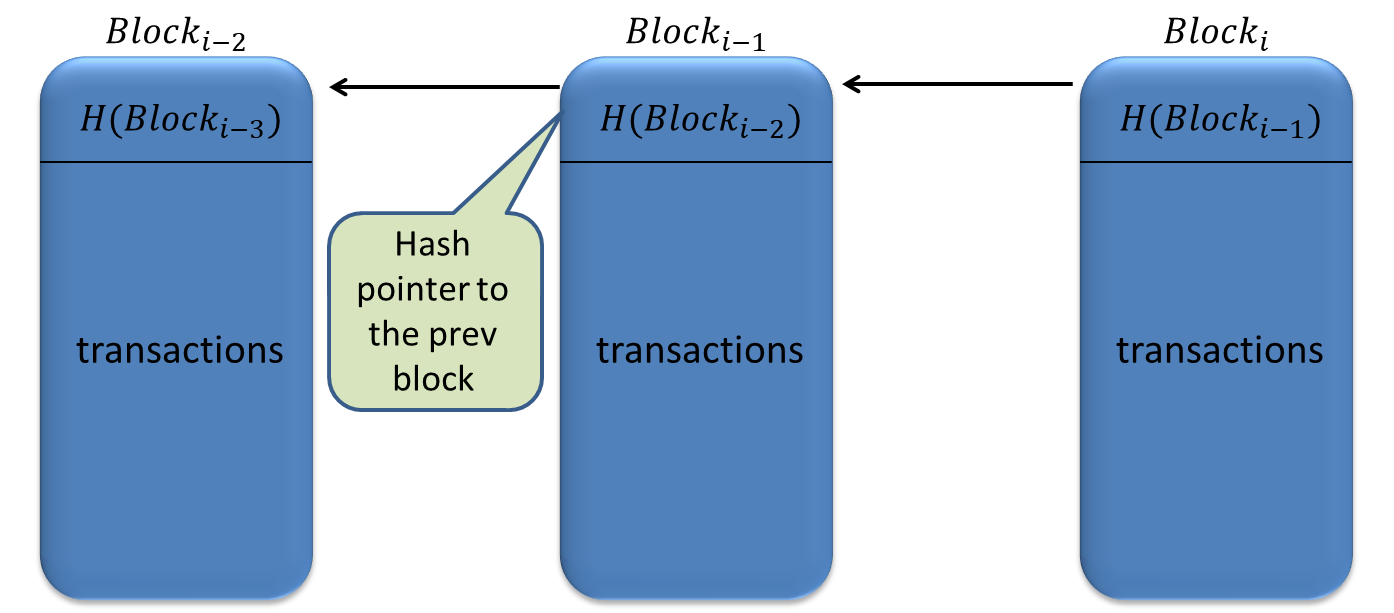
נמשיך בסוף הפרויקט...

**הגדרות**

Block Chain

מבנה נתונים המזכיר linked list , והוא למעשה התשתית לרשת הביטקוין - באמצעותו כל עסקאות הביטקוין מתבצעות. כל Block מכיל:

* Hash pointer – בדומה למצביע "קלאסי", מצביע על הBlock הקודם בשרשרת, אך בנוסף מכיל את ערך תוצאת הHASH של הBlock הקודם. דבר זה מאפשר את אימות המידע הקיים בBlock הקודם.
* Transactions – רשימה המתארת עסקאות המבוצעות ברשת. (ראה ערך Transaction)
* Nonce – הערך אותו הכורה מחשב על מנת לכרות את הBlock. (ראה ערך Bitcoin mining)



Bitcoin Network

רשת הביטקוין מתקשרת במודל של Peer to Peer , כלומר כל node ברשת הביטקוין יכול לשלוח הודעה לכל node אחר ברשת. כך כל node מחזיק בעותק משלו של הBlock Chain וברגע בו יש עדכון בשרשרת הוא מפיץ זאת לכל שאר ה- nodes ואלו שומרים את העדכון בעותק הנמצא אצלם.

Transaction-

כל טנרזקציה ברשת הביטקוין היא למעשה רישום של העברת סכום של מטבעות ממשתמש למשתמש על גבי הBlock Chain באופן הבא: המוען מספק Hash pointer לעסקה בה הוא קיבל את המטבעות, את כמות המטבעות אותה ברצונו להעביר (לא בהכרח מספר שלם) ואת הנמען אליו הוא רוצה להעביר את המטבעות, ואת היתרה המוען מעביר לעצמו. כל עסקה נחתמת דיגיטלית ע"י המשלם על מנת להבטיח את אמינותה של העסקה.

Bitcoin mining-

כריית Bitcoin היא למעשה הוספת Block חדש לBlock Chain, כאשר כורה רוצה להוסיף Block חדש עליו לוודא את נכונות ה- Block הקודם, כלומר הכורה מוודא בתהליך הכרייה כי מתקיימים התנאים הבאים:

* Hash Pointer תקין, ואכן מתאים לHash של ה- Block הקודם.
* ב- Block הקודם כלל הטרנזקציות תקינות על ידי מעבר על כל טרנזקציה ווידוא שכל מוען אכן קיבל בעסקאות קודמות את סך המטבעות אותו הוא מעביר.
* תקינות ה- Nonce של הבלוק הקודם.

על הכורה לאסוף טרנזקציות שטרם נכנסו לשרשרת ולוודא את תקינותן, וכן עליו לפתור פאזל. אם ה- Block הקודם לא עובר את בדיקות התקינות הכורה ילך אחורה בשרשרת עד שימצא Block תקין ואליו יוסיף את ה- Block החדש. בדיקה זאת מבטיחה את "בריאותו" ותיחזוקו הנכון של הBlock Chain.

נציין כי במידה ולכורה יש אפשרות להוסיף את ה- Block שלו לכמה בלוקים במקביל, יש לבחור בענף הארוך ביותר, ורק הטרנזקציות הנמצאות על הענף הארוך ביותר תקפות.

עבור מלאכה זו הכורה מקבל "פרס" , פרס זה הוא בעצם טרנזקציה של מטבעות ללא מוען והנמען הוא הכורה.

סכום העברה בו זוכה הכורה משתנה לאורך חיי ה- Bitcoin כך שבשנת 2009 הסכום עמד על 50 Bitcoin ואחרי כל 210,000 בלוקים ( בקירוב 4 שנים ) מצטמצם ה"פרס" בחצי. הפאזל שעל הכורה לפתור הוא , כלומר עליו למצוא Nonce שתוצאת פונקציית הHash עליו משורשר עם הבלוק תיתן תוצאה שקטנה מ- N.

N משתנה בהתאם לכוח החישוב הפועל ברשת ונקבע בצורה כזאת שבממוצע כל 10 דק' יתווסף בלוק חדש לBlock Chain, לכן ככל שיותר אנשים מנסים לכרות Bitcoin ערכל של N יותר קטן, והפאזל יותר קשה לפתרון . הדרך לחישוב N היא: , כלומר כל 2016 בלוקים (כשבועיים) ערכו של N ובהתאם רמת הקושי לפתרון מתעדכנת בהתאם לכוח החישוב ברשת.

**פיצולים ברשת ה- Bitcoin**

היות וה- Bitcoin הוא תוכנה המבוססת על קוד פתוח , כל עדכון תוכנה צריך להתבצע בכל ה- Nodes ברשת, אולם בגלל עיקובים ברשת ו/או חוסר הסכמה של משתמשים לגבי נהלי הרשת עלולים להיווצר פיצולים ברשת.

נחלק את הפיצולים האפשריים ברשת לשני חלקים:

* **Soft fork** - כאשר עדכון התוכנה מבצע "הקשחה" של הכללים לפיהם בלוק נחשב לתקין, במצב זה Nodes שמריצים את הגרסה הישנה יקבלו בלוקים במבנה החדש, אך Nodes שמריצים את הגרסה הישנה לא יקבלו בלוקים במבנה הישן. היות וכל הNodes מקבלים בלוקים הנוצרו בגרסה החדשה, רוב כוח החישוב ברשת תומך בבלוקים אלו. לכן מובטח כי הענף הארוך ביותר יהיה זה עם הבלוקים הכתובים בגרסה החדשה. כך לא יווצר Hard fork, אלא כמה פיצולים קטנים עד אשר כל ה- Nodes יעדכנו את הגרסה שהם מריצים.

Old  
Version

Old  
Version

New  
Version

Old  
Version

New  
Version

* **Hard fork** - כאשר מתבצע עדכון אשר משנה את מבנה ה- Block המקובל או את תוכנו, כך שהגרסה הקודמת תזהה בלוק זה כלא תקין. מתוך כך יווצר ענף בשרשרת הפועל על הגרסה החדשה וענף הפועל על הגרסה הישנה.  
  עדכון תוכנה מסוג זה מצריך הסכמה של רוב המשתמשים ברשת ה – Bitcoin. משתמשים הבוחרים להישאר בגרסה הישנה עושים זאת בעיקר משיקולים כלכלים ( למשל: בעלים של חומרה יעודית המתאימה לגרסה הישנה של המטבע).

**…**

Bitcoin

Bitcoin

Bitcoin

Bitcoin

Bitcoin

Cash

Bitcoin

Cash

**…**

Bitcoin Pizza Fork**ההיסטוריה של הפיצולים**

|  |  |  |
| --- | --- | --- |
| **Fork Block** | **Fork date** | **Fork name** |
| 478559 | 1.8.2017 | Bitcoin Cash |
| 491407 | 10.10.2017 | Bitcoin Gold |
| 501888 | 1.12.2017 | Bitcoin Nano |
| 498888 | 12.12.2017 | Super Bitcoin |
| 501888 | 1.1.2018 | Bitcoin Pizza |
| 516095 | 1.4.2018 | ClassicBitcoin |

**מטרת הפרויקט**

תכנון ,עיצוב ובניה של מערכת מבוססת WEB, שמטרתה היא לעזור למשתמשים ברשת ה- Bitcoin לקבל מידע אודות מטבעות "אבודים" שאותם הרוויחו מפיצול במטבע לגרסאות שונות עקב Hard Forks שהתרחשו במהלך חיי המטבע.  
הפרויקט ינגיש מידע בסיסי אודות מטבע ה- Bitcoin והרשת על גביה הוא פועל, וכן מידע על תהליך הפיצול של המטבע.   
על המערכת להיות User Friendly ולספק חווית משתמש נוחה כך שתמשוך אליה משתמשים רבים.  
איתור ומימוש אלגוריתם חיפוש יעיל אשר יניב תוצאות חיפוש מהירה בריצה על רשת ה – Bitcoin.

**אנקדוטות** נראה מה נעשה עם זה

* ערך המטבע הקטן ביותר שניתן להעביר על גבי רשת הביטקוין הוא SATOSHI יחיד שערכו הוא Bitcoin.
* ערכו של Bitcoin בודד בשנת 2009 עמד על כ0.05$ , והגיע לשיא בסוף שנת 2017 וערכו עמד על 17,600$.
* כיום כריית ביטקוין ע"י מחשב ביתי כמעט ואינה אפשרית, למחשב ביתי בעל CPU ממוצע יקח מאות אלפי שנים לכרות בלוק(Narayanan, 2016).
* שכמות הביטקוין הנכרת מצטמצת בחצי כל 210,000 בלוקים, הכמות הכללית של ביטקוין הקיימת ברשת היא סדרה הנדסית מתכנסת. כלומר כמות הביטקוין היא סופית ותגיע לכ21 מילון.

**שאלות לרן**

1. אלגוריתם חיפוש – האם לחפש מתחילת השרשרת או מזמן שיתנו לנו
2. חייב חיפוש מהג'נסיס או שאפשר לרוץ אחורה על עסקאות?
3. כמה פיצולים לכלול?
4. מה זה הפיצולים שהתחילו בNODE 0 (ג'נסיס)

**שאלות לעצמנו**

1. בחירת טכנולוגית עבודה
2. החזקת שרת / משיכה משרת קיים
3. שפות תכנות
4. כמות דפים באתר

**בבילוגרפיה**

* Narayanan, Bonneau, Felten, Miller and Goldfeder.***Bitcoin and Cryptocurrency Technologies****, 2016. Princeton University Press.*
* Information regarding Retrieved from:

<https://www.blockchain.com/>

# CryptoPotato. (2018). ***.הפיצולים ברשת הביטקוין 2018: מה חשוב לדעת*** Retrieved from:<https://cryptopotato.com/>

* Forks. (2018). ***Bitcoin Forks*.** Retrieved from:

<https://www.forks.net/list/Bitcoin/>