digital whisper
Technologic Papers

Bitcoin - כסף דיגיטלי ב-P2P

מאת: ד"ר אריק פרידמן

"The chief value of money lies in the fact that one lives in a world in which it is overestimated."

H.L. Mencken

הקדמה

בשנתיים האחרונות הגיח סוג חדש של מטבע. מטבע שמאיים להפוך על-פיהם את סדרי הכלכלה העולמית ולשבור את התלות בממשלות ובנקים בכל הנוגע להעברת כספים בין פרטים. הביטקוין.

הביטקוין הוא כסף דיגיטלי. הרעיון של כסף דיגיטלי כשלעצמו אינו חדש, ונחקר כבר למעלה מ-20 שנה (ייצוג דיגיטלי של כסף אמיתי הוא כמובן ותיק בהרבה). יתר על כן, מטבעות דיגיטליים נמצאים כבר בשימוש נרחב, למשל נקודות מיקרוסופט לרכישת משחקי XBOX, או Facebook Credits לביצוע עסקאות בפייסבוק. החידוש והייחוד של ביטקוין הוא שמדובר במטבע שאין אף גוף מרכזי ששולט או מפקח עליו, אלא הוא מנוהל על-ידי מערכת Peer to Peer. לאי-תלות זו יש מספר השלכות מעניינות. ראשית, הצורך במתווכים (בנקים) לביצוע עסקאות במערכות המסורתיות כרוך בעמלות, שמייקרות את עלות העסקאות. עלות זו הופכת להיות בעייתית במיוחד כשמדובר בעסקאות קטנות (מיקרו-תשלומים). שנית, במערכות המסורתיות אין יכולת לבצע תשלומים לא הפיכים תמורת שירותים שאינם הפיכים, אלא אם נעשה שימוש בכסף פיסי. הונאות הן חלק מהמשחק, ותמיד יש סיכון שהעסקה לא תכובד (צ'ק שחוזר, עסקת אשראי שבוטלה). מערכת הביטקוין מבטיחה לתת מענה לבעיות אלה, תוך התבססות על כלים קריפטוגרפיים וללא צורך באמון בגורם צד ג' כגון בנק או חברת אשראי. אחד האתגרים הגדולים במערכת כזו הוא למנוע שימוש כפול במטבע (כלומר תשלום עם אותו מטבע ביותר מעסקה אחת בו זמנית). במאמר זה נבחן כיצד עובדת מערכת ביטקוין, וכיצד היא מתמודדת עם הונאות.

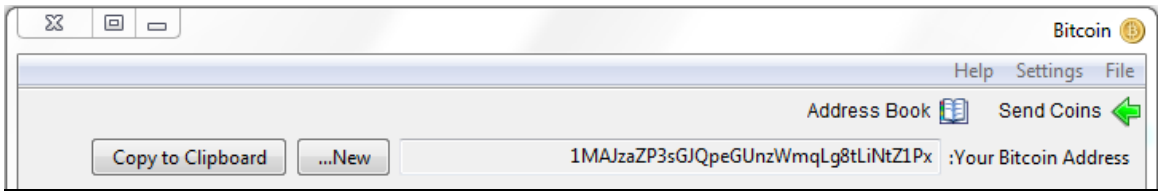
המאמר מניח כי הקורא מכיר את המושגים של מפתחות פרטיים וציבוריים, חתימות דיגיטליות, ופונקציות תמצות קריפטוגרפיות. המעוניינים במידע על מפתחות ציבוריים וחתימות יכולים לקרוא את המאמר של הלל חימוביץ' בנושא בגליון 3, והנושא של פונקציות תמצות קריפטוגרפיות תואר במאמר של ד"ר אור דונלקמן בגליון 21.

מאיפה הגיע BitCoin?

המערכת של ביטקוין החלה לעבוד ב-2009. לא ידוע מי מקים המערכת - הוא השתמש בשם הבדוי סטושי נקמוטו (Satoshi Nakamoto) וטען שהוא מיפן (אם כי נראה שיש לו שליטה מעולה באנגלית, ולא נראה שימוש ביפנית באתר או בקוד של ביטקוין). סטושי פרסם את עקרונות המערכת במסמך טכני, ובמקביל האתר של ביטקוין ספק את התוכנה עצמה ופרטים נוספים. עם זאת, אין צורך להסתמך על מהימנותו של סטושי כדי לבטוח בביטקוין. התוכנה של ביטקוין מנוהלת כתוכנת קוד פתוח, וכל אחד יכול לגשת לאתר של ביטקוין ב-Sourceforge, להוריד את הקוד, לבחון אותו, ולהדר אותו בעצמו.

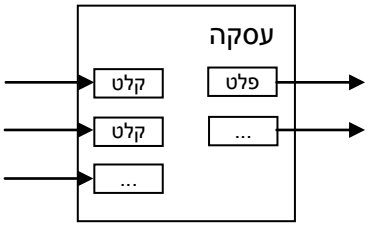
מי יכול להשתמש ב-BitCoin?

כל אחד יכול להשתמש בביטקוין. כל מה שנדרש הוא להוריד את התוכנה של ביטקוין מהאתר של ביטקוין, ואפשר להתחיל לקבל ולבצע תשלומים בביטקוין. מאחר ואין גוף מרכזי שמנהל את המערכת, אין צורך לפתוח חשבון או להזדהות. עם התקנת התוכנה, מוקצה למשתמש זוג מפתחות ציבורי-פרטי חדש, "כתובתו" של המשתמש נגזרת ישירות מהמפתח הציבורי שלו, וניתן להשתמש בה כיעד לתשלום. המשתמש יכול לייצר לעצמו מפתחות נוספים כאוות נפשו. למעשה, התוכנה של ביטקוין מעודדת זאת, וכאשר מתקבל תשלום בכתובת של המשתמש, התוכנה תייצר מייד מפתחות חדשים (וכתובת חדשה) לשימוש לעסקה הבאה. באופן זה, יהיה קשה לקשר עסקאות שונות שביצע אותו המשתמש, אם נעשו באמצעות כתובות ביטקוין שונות.



תוכנת ביטקוין היא תוכנת P2P, והיא מוצאת משתתפים אחרים ברשת באמצעות חיבור לשרת IRC (ערוץ #bitcoin בשרת irc.lfnet.org). במידה ולא הצליחה לייצר קשר כזה, נעשה שימוש ברשימת משתתפים הכלולה בקוד התכנית, ודרכם ניתן ליצור קשר עם משתתפים נוספים.

ביטקוין היא למעשה מערכת לעיבוד עסקאות, והן מהוות את לב המערכת. לכל עסקה יהיו קלטים ופלטים:



הקלטים הם עסקאות קודמות, המגדירות סכומי מטבעות המשמשים בעסקה החדשה, והפלטים הם סכומי המטבעות המוקצים למשתתפים בעסקה (ומהווים בסיס לעסקאות עתידיות). בדרך כלל יהיו שני פלטים: אחד עבור הקצאת סכום למוטב בעסקה, ואחד כדי לייצג את העודף למבצע העסקה. ברוב העסקאות סכום המטבעות בקלט וסכום המטבעות בפלט יהיו שווים, אולם יש גם סוג מיוחד של עסקאות המשמשות ל"הטבעת" מטבעות חדשים, נושא שיפורט בהמשך. למשל, להלן עסקת הטבעת מפתחות:


```
{
  "hash":"f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
  "ver":1,
  "vin sz":1,
  "vout sz":1,
  "lock time":0,
  "size":134,
  "in":[
    {
      "prev out":{
        "hash":"0000000000000000000000000000000000000000000000000000000000000000",
        "n":4294967295
      },
      "coinbase":"04e6ed5b1b015c"
    }
  ],
  "out":[
    {
      "value":"50.00000000",
      "scriptPubKey":"04283338ffd784c198147f99aed2cc16709c90b1522e3b3637b312a6f9130
       e0eda7081e373a96d36be319710cd5c134aaffba81ff08650d7de8af332fe4d8cde20 OP_CHECKSIG"
    }
  ]
}
```


כעסקה להטבעת מטבע חדש אין לה קלטים (prev_out מאופס), ויש לה פלט אחד, המקצה 50 ביטקוין לבעל המפתח הפומבי שמתחיל ב-...04283. העסקה מיוצגת באמצעות התמצות שלה, המתחיל ב-f5d8ee... ומופיעה בתחילתה.

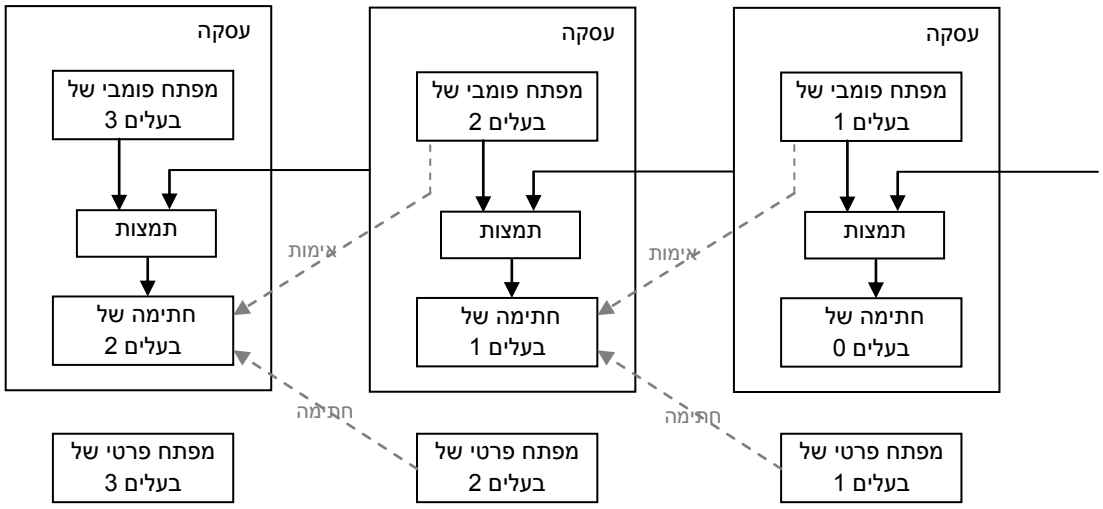
להלן עסקת העברת כספים:


```
{
  "hash":"5a4ebf66822b0b2d56bd9dc64ece0bc38ee7844a23ff1d7320a88c5fdb2ad3e2",
  "ver":1,
  "vin_sz":1,
  "vout_sz":1,
  "lock_time":0,
  "size":158,
  "in":[
    {
      "prev_out":{
        "hash":"f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6",
        "n":0
      },
      "scriptSig":"304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
      90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501"
    }
  ],
  "out":[
    {
      "value":"50.00000000",
      "scriptPubKey":"OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
      OP_EQUALVERIFY OP_CHECKSIG"
    }
  ]
}
```


ניתן לראות כי הקלט לעסקה הזו הוא העסקה הקודמת (שערכה 50 ביטקוין), ויש לה פלט יחיד המקצה את כל 50 הביטקוין למשתמש שתמצות המפתח הפומבי שלו מתחילה ב-...40437.

למעשה, עסקאות אלה *מגדירות* את המטבעות ואת בעליהם. באופן כללי, כל מטבע מוגדר על-ידי סדרת עסקאות, הראשונה בהן היא עסקת הטבעת המטבע, ואחריה יש שרשרת של עסקאות המתארות את שרשרת הבעלות על המטבע. כדי להעביר מטבע, בעל המטבע מייצר עסקה חדשה. עסקה זו תכלול את התמצות של העסקה הקודמת (כלומר, ממשיכים את שרשרת הבעלות) ואת המפתחות הפומביים של נותן המטבע ומקבל המטבע, והיא תהיה חתומה על-ידי הבעלים של המטבע. קיימת אפשרות גם להציע עמלה עבור עיבוד העסקה (פרטים בהמשך). התהליך מתואר בתרשים בעמוד הבא. כיוון שרק לבעלים החוקיים יש את המפתח הפרטי המתאים למפתח הפומבי בעסקה האחרונה בשרשרת, הוא היחיד שמסוגל לייצר חתימה תקינה ובכך להכריז על העסקה. עם זאת, העסקה החתומה מהווה רק ראייה ראשונית (אם כי עדיין לא מספקת, כפי שנראה) לכך שהועברו המטבעות.

אם כך, עסקאות ביטקוין מאפשרות לייצר מטבעות ולהעביר אותם מיד ליד. אבל מה בעצם מונע מכל אחד לייצר מטבעות כאוות נפשו? או להשתמש באותו מטבע פעמיים באמצעות יצירת שתי עסקאות שונות על-בסיס אותה עסקה קיימת? התשובה טמונה בתהליך עיבוד העסקאות של ביטקוין, המתבסס על יצירת *בלוקים* של עסקאות.



עיבוד עסקאות BitCoin - בלוקים והוכחת עבודה

כאשר מישהו מייצר עסקת ביטקוין וחותם עליה עם המפתח הפרטי שלו, הוא מכריז על נכונותו לבצע את התשלום, אולם העסקה לא תקפה עד שמסה קריטית של משתתפים במערכת ה-P2P של ביטקוין מכירים בעסקה ומקבלים אותה. הדרך שבה עסקאות נבחנות ומתקבלות על-ידי המשתתפים במערכת היא באמצעות תהליך עיבוד *בלוקים* של עסקאות. היסטוריית העסקאות של ביטקוין מתוחזקת על-בסיס שרשרת יחידה המורכבת מבלוקים, כאשר כל בלוק מכיל עסקה אחת או יותר. נכון לזמן כתיבת שורות אלה, השרשרת מכילה 142,620 בלוקים. הבלוק הראשון בשרשרת (בלוק 0) נקרא בלוק בראשית (The Genesis block), והוא נראה כך:

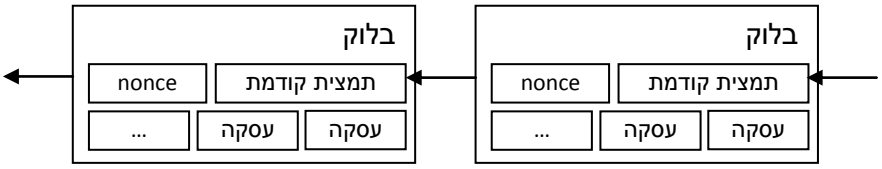

```
{
  "hash":"000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f",
  "ver":1,
  "prev_block":"0000000000000000000000000000000000000000000000000000000000000000",
  "mrkl_root":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
  "time":1231006505,
  "bits":486604799,
  "nonce":2083236893,
  "n_tx":1,
  "size":285,
  "tx":[
    {
      "hash":"4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b",
      "ver":1,
      "vin_sz":1,
      "vout_sz":1,
      "lock_time":0,
      "size":204,
      "in":[
        {
          "prev_out":{
            "hash":"0000000000000000000000000000000000000000000000000000000000000000",
```

```
            "n":4294967295
          },

"coinbase":"04ffff001d0104455468652054696d65732030332f4a616e2f32303039204368616e63656c6c6f
72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73"
        }
      ],
      "out":[
        {
          "value":"50.00000000",

"scriptPubKey":"04678afdb0fe5548271967f1a67130b7105cd6a828e03909a67962e0ea1f61deb649f6bc3f
4cef38c4f35504e51ec112de5c384df7ba0b8d578a4c702b6bf11d5f OP_CHECKSIG"
        }
      ]
    }
  ],
  "mrkl_tree":[
    "4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b"
  ]
}
```


הבלוק הזה כולל עסקה אחת (50 הביטקוין הראשונים שנוצרו). הקוד של ביטקוין כולל את הבלוק הזה, כך שכל לקוח ביטקוין מסוגל לוודא ששרשרת הבלוקים מתחילה בבלוק הבראשית. כל בלוק נוסף בשרשרת כולל את התמצית של הבלוק שלפניו, עסקה אחת או יותר, ערך מספרי בשם nonce (פרטים בהמשך), ותמצית של ערכי הבלוק. כך נוצרת השרשרת הבאה:



שרשרת בלוקים חוקית חייבת להתחיל בבלוק הבראשית, אולם ניתן לייצר יותר משרשרת אחת כזאת. במקרה ומשתתפים ברשת מכריזים על יותר משרשרת חוקית אחת במערכת, מערכת ביטקוין (כלומר האוסף של המשתתפים החברים בה) תמיד תיקח את השרשרת הארוכה ביותר. כפי שנראה בהמשך, יש צורך בהשקעת משאבים חישוביים ניכרים לצורך יצור שרשרת חוקית. במידה וגורם זדוני כלשהו ירצה לשכתב את היסטוריית העסקאות ולספק שרשרת חלופית, הוא יצטרך לספק שרשרת ארוכה יותר מהשרשרת הקיימת. משימה זו תדרוש שיהיה ברשותו כוח חישובי העולה על זה של כל שאר המשתתפים במערכת ביחד. במידה ואין לו כוחות חישוביים כאלה, זיוף שרשראות הופך להיות משימה בלתי אפשרית מכל בחינה מעשית. במידה ונוצר מצב ואכן לגורם כלשהו יש שליטה על רוב הכוחות החישוביים במערכת, הרי שכל הנראה יוכל להרוויח יותר על-ידי עיבוד עסקאות ויצירה של בלוקים "לפי הספר", מאשר באמצעות רמאות שתגרום לאובדן אמון במערכת ובריחת המשתתפים. באופן זה המערכת מתוכננת לתמוך בביצוע מהימן של עסקאות המשתתפים.

```
"How can you have money," demanded Ford, "if none of you actually
produce anything? It doesn't grow on trees you know."
"If you would allow me to continue…"
Ford nodded dejectedly.
"Thank you. Since we decided a few weeks ago to adopt leaves as legal
tender, we have, of course, all become immensely rich."
Ford stared in disbelief at the crowd who were murmuring appreciatively
at this and greedily fingering the wads of leaves with which their track
suits were stuffed.
"But we have also," continued the Management Consultant, "run into a
small inflation problem on account of the high level of leaf
availability, which means that, I gather, the current going rate has
something like three major deciduous forests buying one ship's peanut."
Murmurs of alarm came from the crowd. The Management Consultant waved
them down.
"So in order to obviate this problem," he continued, "and effectively
revalueate the leaf, we are about to embark on a massive defoliation
campaign, and… er, burn down all the forests. I think you'll all agree
that's a sensible move under the circumstances."
```

(Life, the Universe and Everything, Douglas Adams)

כפי שיתואר בהמשך, יצור בלוק כרוך בעבודה חישובית, והמערכת מכוונת לייצר בלוק חדש בערך כל 10 דקות. העסקה הראשונה (ולעיתים היחידה) בכל בלוק תהיה תמיד עסקה המעניקה מטבעות ביטקוין ליוצר הבלוק כשכר על העמל החישובי. חלק משכר זה מגיע ממטבעות חדשים שנוצרים (כלומר העסקה הראשונה היא עסקת הטבעת מטבעות), וחלקו מגיעים מעמלות שמציעים מייצרי העסקאות. הקוד של ביטקוין נכתב כך שב-4 השנים הראשונות, כל בלוק חדש ייצר 50 ביטקוין (כך שיווצרו 10,500,000 מטבעות בתקופה זו). כמות זו תחולק בחצי כל 4 שנים, כך שבשנים 4-8 יתקבלו 25 ביטקוין על כל בלוק (עם 5,250,000 מטבעות חדשים בתקופה), בשנים 8-12 יתקבלו 12.5 ביטקוין וכן הלאה. לאורך זמן, כמות המטבעות הכוללת תתקרב ל-21,00,000, ואף פעם לא תעבור את רף זה - בשנת 2140 התשלום במטבעות חדשים על יצירת בלוק יאופס. תכנון זה של המערכת צופה שבשלבי החיים המאוחרים יותר של המערכת העלות של עיבוד העסקה תכוסה בעיקרה על-ידי העמלות שמציעים מייצרי העסקאות, והצורך בתמריץ של מטבעות חדשים יפחת. כמו-כן, במערכת כזו לעולם לא תהיה אינפלציה - יש חסם עליון וקשיח לכמות הכסף שיווצר.

אחד המרכיבים המרכזיים במערכת ביטקוין הוא העקרון של הוכחת עבודה (Proof of work). עקרון זה הוצע במקור ב-1997 על-ידי אדם בק, בהקשר של מערכת hashcash למניעת ספאם. הרעיון היה שכל משלוח דואר אלקטרוני יצריך את השולח לספק הוכחה לכך שהשקיע כמות מסויימת של משאבי עיבוד בשליחת ההודעה, למשל, חישוב שיצריך זמן עיבוד של שתי שניות. עבור משתמשים רגילים, זה לא היה משפיע באופן מהותי, שכן עיכוב של שתי שניות יהיה כמעט ובלתי מורגש מבחינתם. לעומת זאת, עבור

ספאמרים השולחים מליונים של תכתובות אלקטרוניות תידרש השקעה משמעותית של זמן וכסף, דבר שיהפוך את עסקי הספאם ללא כדאיים. בדיעבד, שיטה זו התבררה כלא מוצלחת למניעת ספאם, בעיקר מפני ששימוש בה היה פוגע גם בגופים השולחים כמויות גדולות של דואר לגיטימי. אולם הרעיון יושם בהצלחה במסגרת המערכת של ביטקוין.

על מנת שבלוק יהיה חוקי, עליו לקיים את התנאי הבא: התמצית של הבלוק צריכה להיות קטנה מערך מטרה מסויים, המוסכם על-ידי המערכת. במילים אחרות, התמצית של הבלוק צריכה להתחיל בשרשרת של אפסים. המפתח ליצירת תמצית כנדרש טמון במחרוזת ה-nonce הנמצאת בבלוק. תהליך יצירת בלוק חדש מתבצע באופן הבא:

1. מצא את שרשרת הבלוקים החוקית הארוכה ביותר במערכת.
2. הגרל מחרוזת nonce. יצר בלוק חדש המורכב מתמצית הבלוק האחרון בשרשרת, מהעסקאות הממתינות לעיבוד (כולל עסקת יצירת מטבעות המעניקה תשלום למייצר הבלוק) ומה-nonce.
3. אם ערך התמצית של הבלוק החדש מתחיל במספר האפסים הדרוש, פרסם את הבלוק.
4. אחרת חזור ל-2 עם nonce אחר.

אם בשלב כלשהו בתהליך תפורסם שרשרת בלוקים חוקית ארוכה יותר (כלומר מישהו הצליח לחשב את הבלוק הבא), אז תהליך יצירת הבלוק יעבור להתבסס על שרשרת זו. במידה ומישהו מנסה לייצר בלוק שאינו עומד בכללים של המערכת (למשל, אי-התאמה בחישובי תמצות, חריגה מסכום הכסף שמגיע למייצר הבלוק), הבלוק יידחה על-ידי שאר המשתתפים ברשת, וכך יימנעו רמאויות.

ערך המטרה של התמצית, או מספר האפסים הדרושים, נקבע על-פי הזמן שלקח לייצר את 2016 הבלוקים הקודמים. המטרה היא להתאים את רמת הקושי של הבעייה החישובית לכמות המשאבים החישוביים הקיימים ברשת, כך שבממוצע יווצר בלוק חדש כל 10 דקות.

באתר http://blockexplorer.com ניתן לעקוב אחר ייצור הבלוקים, ולראות את כלל היסטוריית הבלוקים (והעסקאות) עד כה.

בימים המוקדמים יותר של המערכת, תוכנת ביטקוין כללה את האפשרות להשתתף בתהליך עיבוד הבלוקים, ומכאן גם את היכולת לזכות במטבעות ביטקוין. אולם עם התפשטות המערכת ועליית הערך של ביטקוין, חל תהליך של התמחות ביצור מטבעות. למשל, כרטיסים גרפיים יכולים לכרות מטבעות בקצב מהיר פי 100 ויותר מאשר מעבד מחשב רגיל. התמריץ לייצור מטבעות עלה, והחלו להופיע חוות לכריית ביטקוין. למעשה, צריכת החשמל של חוות כריית ביטקוין מזכירה את זו של חממות לגידול מריחואנה, וכבר דווח על מקרים שמשטרה פרצה לבתים במטרה למצוא מגדלי סמים ומצאה גיקים עם מחשבים.

בנוסף, משתתפים החלו להתאגד לכרייה משותפת של מטבעות (pools), ויצרו קבוצות כגון deepbit, slush ו-btcguild.

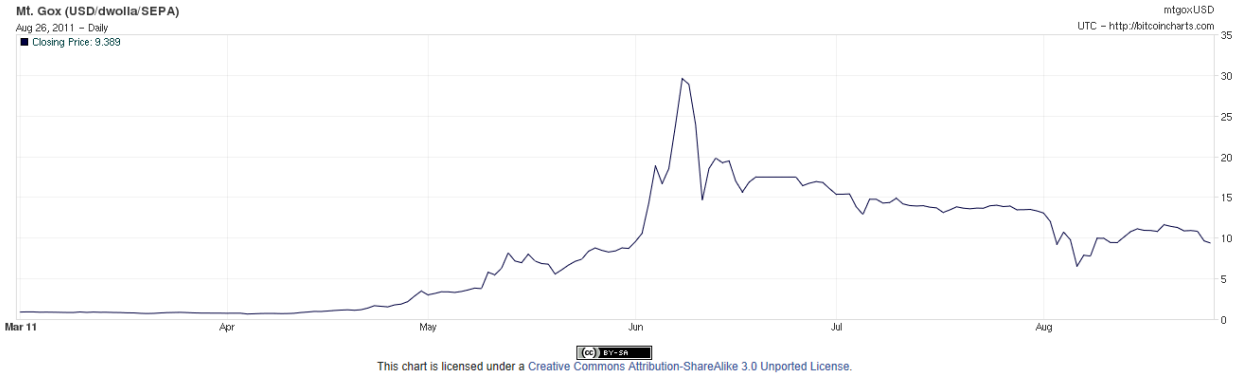
עם גדילת משאבי החישוב ברשת, רמת הקושי של הבעייה החישובית עלתה (נכון לכתיבת שורות אלה דרושה בתמצית תחילית של 52 אפסים). מאחר ובמצב הנוכחי עלות כריית הביטקוין תשתלם רק עבור אלה הבונים מערכת ייעודית שתבצע את הכרייה ביעילות, האפשרות לכרייה הוסרה מהתוכנה, ויש צורך להוריד תוכנה ייעודית לכריית ביטקוין.

(מכרה ביטקוין ברוסיה. התמונה נלקחה מ-http://bitcoinitalia.com/forum/viewtopic.php?f=11&t=26)

שווה משהו, ה-BitCoin הזה?

העסקה המתועדת הראשונה בה נרכש פריט פיסי תמורת ביטקוין התקיימה ב-22 במאי 2010. בעסקה זו המשתמש laszlo שילם 10,000 ביטקוין עבור פיצה. באותו זמן ערכם של 10,000 ביטקוין היה בערך 41$. כיום, כעבור שנה ושלושה חודשים, סכום דומה של ביטקוין שווה בערך 100,000$. שעור קטן על חסכון.

עם התפתחות מערכת ביטקוין, החלו לצוץ בורסות (Bitcoin markets) המאפשרות לסחור בביטקוין תמורת מטבעות אחרים. למשל, אחד מהשווקים הבולטים הוא MTgox, וניתן לראות להלן את התנודות בשערי מטבע הביטקוין ביחס לדולר האמריקאי לאורך ששת החודשים האחרונים:



(שער הביטקוין ביחס לדולר האמריקאי. התרשים נלקח מ- http://bitcoincharts.com/charts)

מערכת ביטקוין הייתה על רכבת הרים בתקופה זו, במיוחד לאור החשיפה הגוברת שקיבלה מאז מאי ויוני השנה. בשלב מסויים מטבע הביטקוין נסחר תמורת כ-30$, אולם מאז רמתו ירדה לאזור ה-10$, עדיין הרבה מעל ערכו רק לפני חצי שנה. קיימים גם שווקי מסחר נוספים לביטקוין, וניתן לעקוב אחריהם באתר http://bitcoincharts.com/markets. אתרים נוספים בהם ניתן לעקוב אחר קורותיו של הביטקוין הם http://www.bitcoinmonitor.com ו-http://bitcoinwatch.com. נכון לזמן כתיבת שורות אלה, קיימים כ-7 מליון מטבעות ביטקוין, ששווים הכולל מוערך בכ-68 מליון דולר אמריקאי.

עתידו של ה-BitCoin

לאחר דהירה בערכו של הביטקוין במהלך החודשים מאי ויוני, נראה כי המגמה התהפכה. בעקבות צניחה נוספת בערכו של הביטקוין בתחילת אוגוסט, כתב של הפורבס מיהר להספיד את המטבע, אם כי הירידות נבלמו מאז. כך או כך, עתידו של המטבע הוא נושא לספקולציות.

מצד אחד, מערכת ביטקוין מתמודדת בהצלחה מרשימה עם האתגרים שדורשת מערכת פיננסית בהיקף גדול, ובפרט היכולת להבטיח את מהימנות העסקאות שמבוצעות ומניעת שימוש כפול במטבעות. בנוסף, ההבטחה לעמלות עסקה נמוכות הופכת את ביטקוין למערכת מבטיחה מאוד לאור התגברות הצורך בדרך זולה לביצוע עסקאות קטנות ומיקרו-תשלומים באינטרנט. הצדדים הטכנולוגיים והקריפטוגרפיים של המערכת הופכים אותה לחביבת הגיקים; האנונימיות שנותנת היכולת להתחבא מאחורי מפתח פומבי חסר זהות קורצת לארגונים הפועלים מחוץ לחוק ולאקטיביסטים. שוק הביטקוין עדיין צעיר יחסית, ויכול לספק הזדמנויות מעניינות ליזמים. למשל, השוק עדיין לא לגמרי משוכלל, וניתן לנצל פערי שערים בין שווקי מסחר שונים לארביטרז'.

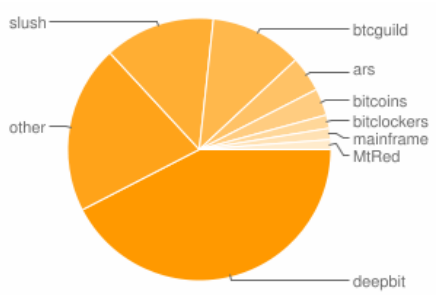
מצד שני, היתרונות של ביטקוין הם גם החסרונות שלה. גופי אכיפת חוק בוחנים את המערכת בחשדנות כמנגנון שעשוי לשמש להלבנת כספים, ואין להוציא מכלל אפשרות שהשימוש במערכת יוצא מחוץ לחוק. למשל, ארגון (Electronic Frontier Foundation) EFF, קבוצה העוסקת בשימור זכויות אזרחיות בעולם הדיגיטלי, אימצה בתחילה את ביטקוין ואיפשרה תרומת ביטקוין לארגון. אולם עם התגברות העניין בביטקוין, הארגון נסוג בו מהחלטתו, בין השאר בשל חוסר הבהירות סביב ההשלכות החוקיות הכרוכות בהקמת מערכת מטבע חדשה, ורצונו של הארגון להתרחק ממעורבות כצד ישיר בעימות אפשרי עתידי סביב המערכת.

מכשול נוסף העומד בדרכה של המערכת הוא רמת הידע והכישורים הגבוהה הנדרשת לשימוש בטוח במערכת. בעלות על מטבעות ביטקוין נשענת כולה על אבטחת המפתחות הפרטיים המתאימים. אובדן של מפתחות אלה (למשל בעקבות קריסת כונן קשיח) או גניבתם על-ידי קוד זדוני, משמעותם אובדן בלתי הפיך של הכספים. למשל, ב-13 ביוני משתמש בשם allinvain דיווח על כך שהמחשב שלו נפרץ ונגנבו ממנו 25,000 מטבעות ביטקוין (שווי-ערך ל-$375,000 בזמן הגניבה). על-פי allinvain, הפורץ הצליח להשיג את המפתח הפרטי שלו, והשתמש בו כדי להעביר אליו את הבעלות על המטבעות. העסקה, כמובן, בלתי הפיכה, ואין אמצעי פשוט למציאת הפושע על-פי המפתח הפומבי בו השתמש כיעד לעסקה. מקרה זה ממחיש כי מערכת ביטקוין, לפחות בצורתה הנוכחית, לא מתאימה לתפוצה מעבר לאוכלוסיית הגיקים, שהינם מתוחכמים מספיק כדי להגן כראוי על קובץ ה"ארנק" בו מאוחסנים המפתחות הפרטיים שלהם; האדם מהרחוב יהווה טרף קל לפושעים מקוונים. בנקים וחברות אשראי מספקים בטחון והגנה

מפני הונאות, וערכם של בטחונות אלה עבור רוב האוכלוסיה משמעותי ומהותי יותר מהיתרונות שמציעה ביטקוין.

סיכום

המגמות של החודשים האחרונים במערכת ביטקוין מעלות תהייה נוספת לגבי עתידה של מערכת כזו. התמריץ הכלכלי הביא למיזוג של משאבי מחשוב, ונכון להיום מספר מצומצם יחסית של גופים שולט ברוב המכריע של משאבי החישוב במערכת. אם מערכת ביטקוין תצליח לשרוד לאורך זמן ולהשיג תמיכה מספיק רחבה כדי לשמור על ערכו של המטבע, גופים אלה יהיו בעמדה לקבוע כרצונם תעריפים לביצוע עסקאות. באופן מעשי, הביטקוין עשוי להפוך ממטבע המתוחזק על-ידי קהילת המשתמשים בו, למטבע המנוהל על-ידי מספר מצומצם של גופים פרטיים. באופן אירוני, ייתכן כי דווקא הצלחת המערכת תביא לעלייה הדרגתית בעמלות הנדרשות (ביכולתם של מייצרי הבלוקים להתעלם מעסקאות המציעות עמלות נמוכות), ובסופו של דבר תחתור נגד אחד הצרכים שהביאו ליצירת המערכת מלכתחילה.



(חלוקת משאבי החישוב ברשת ביטקוין נכון ל-26.8.11 - נלקח מתוך http://bitcoinwatch.com)

בין אם מטבע הביטקוין ימשיך ויתפוס תאוצה, ובין אם העניין בו יתמוסס והוא יגווע, מערכת הביטקוין פרצה דרך חדשה, וממחישה את הצורך והעניין בחלופות לשיטות המסחר המסורתיות. קרוב לוודאי שיש עוד דרך מרתקת בפניה של טכנולוגיה זו.

מקורות ומידע נוסף

המאמר מבוסס בעיקרו על המידע באתר של ביטקוין (http://www.bitcoin.org) ובעיקר עמוד השאלות הנפוצות, ועל המאמר של סטושי נקמוטו, Bitcoin: A Peer-to-Peer Electronic Cash System. אין לראות בשום מידע המובא כאן בגדר המלצה להשתתף או להימנע מלהשתתף במערכת ביטקוין. בעלי ביטקוין שנהנו מקריאת המאמר, יכולים להביע את הערכתם באמצעות תרומה בביטקוין לכתובת MAJzaZP3sGJQpeGUnzWmqLg8tLiNtZ1Px1. ☺

למאזיני פודקאסטים, להלן מספר המלצות חמות נוספות:

1. פרק 98 בפודקאסט *עושים היסטוריה* של רן לוי (ברכות לרגל הפרק ה-100!!) עוסק בהיסטוריה של האינפלציה, ודן גם בביטקוין.
2. פרק 287 בפודקאסט Security Now של סטיב גיבסון מבית TwiT כולל תיאור נרחב של ביטקוין וכיצד המערכת פועלת.
3. פרק 423 בפודקאסט This American Life עוסק בהמצאת הכסף, וממחיש את המסקנה שהכסף הוא אשליה.

על המחבר

ד"ר אריק פרידמן הוא חוקר בתחום של פרטיות ואבטחת מידע, ובעיקר שילובם במסגרת אלגוריתמים ללמידה ממוחשבת וכריית נתונים. אריק סיים את לימודי הדוקטורט בפקולטה למדעי המחשב בטכניון בשנת 2011, והוא מחזיק גם בתואר MBA מאוניברסיטת תל-אביב. עד לאחרונה אריק שילב את המחקר עם תפקיד של Program Manager במיקרוסופט, שם עבד על מוצרים בתחום אבטחת המידע והפרטיות.