

ביטקוין, סייפרפאנק ומשילות במטבעות מבוזרים

נדב איבגי, מייסד Bitrated
nadav@bitrated.com

PGP: FCF1 9B67 8665 62F0 8A43
AAD6 81F6 104C DoF1 50FC

תנועת הסייפרפאנק - Cypherpunk

ARTICLES

SECURITY WITHOUT IDENTIFICATION: TRANSACTION SYSTEMS TO MAKE BIG BROTHER OBSOLETE

The large-scale automated transaction systems of the near future can be designed to protect the privacy and maintain the security of both individuals and organizations.

Communications of the ACM

DAVID CHAUM

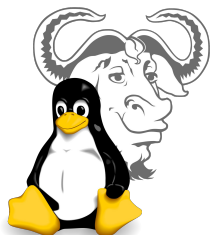
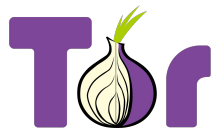
October 1985 Volume 28 Number 10

- תנועה הדוגלת בשימוש בקריפטוגרפיה ככלי לשינוי חברתי-פוליטי והעצמת הפרט אל מול תאגידים וממשלות.

- פועלת לקידום הצפנה להמונים: תקשורת מוצפנת (PGP), טכנולוגיות פרטיות (Tor), הפצה חופשית של מידע (Torrent), כסף דיגיטלי מבוזר (Bitcoin), רשתות Mesh, ועוד.

- 1983: ניצנים ראשונים בעבודה של דיוויד צ'אום על מערכות תשלומים אנונימיות (Ecash).

- 1992: המושג סייפרפאנק נולד, רשימת התפוצה Cypherpunks נוסדת.



"מלחמות הקריפטו"



הימים המוקדמים של הסייפרפאנק אופיינו במאבקים והגדרת גבולות

מגבלות יצוא קריפטוגרפיה מארה"ב

- נכנס לתודעה הציבורית ב 1991 בעקבות PGP והצפנת SSL בנטסקייפ.
- בתחילה אפשרו קריפטוגרפיה חלשה בלבד (40 ביט).
- הפצת קוד תוכנה הוכרה כמוגנת ע"י חופש הביטוי ב 1995. המגבלות הוקלו מאז משמעותית, אבל עדיין קיימות.



החלשת קריפטוגרפיה והחדרת דלתות אחוריות

- Clipper Chip - הוכרז ב 1993, בוטל ב 1996 לאחר מאבק ציבורי נרחב.
- חזר לדיון ציבורי בעקבות הדלפות סנודן (2013) והצפנה של טלפונים חכמים. ניסיונות להוציא הצפנה בלתי פריצה מחוץ לחוק עדיין מתנהלים.

```
#!/bin/perl -sp0777i<X+d*IMLa^*IN%0]dsXx++IMIN/dsM0<j]dsj
$/=unpack('H*',$_);$_=`echo 16dio\U$k"SK$/SM$n\Esn0p[IN*1
IK[d2%Sa2/d0$^Ixp"dc` ;s/W//g;$_=pack('H*',/(.*)*/$)/`
```

כסף דיגיטלי:
עידן ה-BBTC

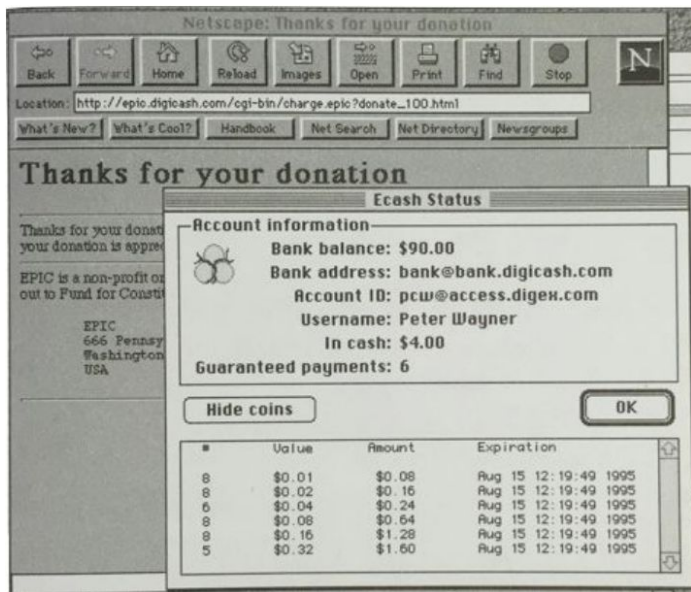
מילטון פרידמן על כסף דיגיטלי, בראיון משנת 1999

(זוכה פרס נובל לכלכלה, 1912-2006)



2006 interview: “I've always been in favor of abolishing the Federal Reserve and substituting a machine program that would keep the quantity of money going up at a steady rate.”

מערכות קריפטו-כסף מוקדמות



Bit gold

A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on [trust in a third party](#) for its value. As many inflationary and hyperinflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs.

- Ecash - דיוויד צ'אום, 1984
מערכת הקריפטו-כסף הראשונה! פרטיות חזקה ובעלות קריפטוגרפית, אבל עם הנפקה וניהול רישום ריכוזיים.
- HashCash - אדם בק, 1997
שימוש בהקרבת משאבים (PoW) כאמצעי למניעת ספאם, שימש כהשראה למערכות כסף, מצוין במאמר של ביטקוין.
- B-money - ווי דאי, 1998
הנפקה מבוססת PoW, עם רישום ריכוזי וללא שליטה באינפלציה, מצוין במאמר של ביטקוין.
- RPOW - האל פיני, 2004
תכונות דומות. מערכת הכסף המבוצרת הראשונה עם קוד!
- Bit-gold - ניק סזאבו, 2006
חם, רותח, לוחט... אבל עדיין לא לגמרי שם.

Bitcoin

Rules without Rulers



מי שולט בביטקוין?

- כלל המשתתפים.
- ספר החשבונאות ציבורי לחלוטין, כולם רואים ומבקרים הכל בזמן-אמת.
- כל משתתף מחליט עבור עצמו תחת איזו מערכת חוקים הוא מוכן להשתתף, ומאמת שהם נאכפים כלשונם באופן עצמאי ובלתי-תלוי.
- אין הגדרה אוניברסלית של "הביטקוין" - תלוי את מי שואלים.
- ניסיון לשנות את החוקים ללא קונצנזוס נרחב יוביל לפיצול ("fork") ויצירת שני מטבעות.
- אוטונומיה מלאה - אף אחד לא יכול לכפות חוקים שאתם לא מוכנים לקבל.

מי שולט בחוקי השחמט?

מערך הכוחות: הכורים

- הכורים נדרשים לעמוד בחוקי הפרוטוקול של הרשת. שינוי החוקים משמע יצירת מטבע חדש.
- המשתמשים: "אנחנו מוכנים לקנות את המטבעות שתייצרו אם תפעלו תחת החוקים שאנחנו הגדרנו".
- תוקף 51% יכול לעשות שלושה דברים בלבד: למנוע מטרנזקציות לקבל אישור, למנוע מכורים אחרים לכרות בלוקים, ולבטל תשלומים שהוא שלח.
- הוא לא יכול לייצר "מטבעות מהאוויר", לקחת מטבעות שלא שייכים לו, או לשנות את חוקי הפרוטוקול בדרך כלשהי.
- נשק יום הדין: החלפת פונקציית proof-of-work ("לפטר את המיינרים").



מערך הכוחות: ארנקים ובורסות



- לסט החוקים שהבורסות והארנקים מגדירים כביטקוין יש חשיבות רבה: הם הגופים העיקריים שמתמשים סומכים עליהם להרצת צומת מלאה.

- אבל: גם הם בסופו של דבר תלויים במשתמשים ובסוחרים, ונמצאים בסביבה תחרותית.

- אם הם יבחרו בסט חוקים שהמשתמשים לא רוצים, המשתמשים יעזבו לטובת מתחרים.



מערך הכוחות: המפתחים

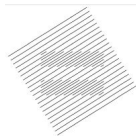
- המפתחים כותבים את הקוד, אבל משתתפי רשת צריכים להסכים לאמץ ולהריץ אותו בפועל.
- הכוח של המפתחים מוגבל ע"י מנגנון בלמים ואיזונים שמופעל ע"י כלל משתתפי המערכת.
- המשתמשים יכולים לבחור מבין גרסאות הקוד של קבוצות פיתוח אלטרנטיביות.
- עם זאת: חשוב שתהליכי הפיתוח הפנימיים בקהילת הפיתוח יתנהלו בצורה שתבטיח יציבות ושקיפות, ותמזער את הסכנה של פיצול הרשת.

קהילת פיתוח הביטקוין

 BitcoinCore



Bitcoin-S



 bitcoinj

bitcore



bcoin Bitcoin F#

NBitcoin conformal



- קהילה בינלאומית של מאות מפתחים ומדענים שעובדים במבנה שטוח, ללא היררכיה וללא מקבלי החלטות.
- תפקיד המפתח הראשי הוא סמלי ובעיקרו לוגיסטי.
- 12 הטמעות של ביטקוין ב 9 שפות שונות. שיתוף פעולה על פיתוח הפרוטוקול תחת תהליך העבודה של ביטקוין קור.
- מוקד משיכה למומחי קריפטוגרפיה, אנשי אקדמיה וחוקרי אבטחה מובילים בתחומם.
- קצב פיתוח, מחקר וחדשנות פנומנליים!

עקרונות מנחים בפיתוח ביטקוין

- קבלת החלטות מונחית קונצנזוס ותהליך מדעי של ביקורת עמיתים.
- שימור הסטטוס קוו תמיד עדיף על פני שינויים מעוררי מחלוקת - גם במחיר של התקדמות איטית. קושי לשנות את ביטקוין זו תכונה רצויה.
- חשיבות הגנה על תכונות הליבה של ביטקוין - גם מפני עריצות הרוב.
- תקשורת ציבורית ושקופה. החלטות מתקבלות בדיון אונליין מתועד בלבד.
- השתתפות פתוחה, הצעות נבחנות על סמך שיקולים טכניים.
- "First, do no harm" - שמירה על יציבות המערכת מעל הכל, התנהלות זהירה וקונסרבטיבית, בדיקות ותהליכי QA קפדניים.

הטכנולוגיה היא רק כלי

nadav@bitrated.com

PGP: FCF1 9B67 8665 62F0 8A43
AAD6 81F6 104C D0F1 50FC