הלבנת הון בביטקוין: כיצד ניתן להעלים מידע במאגר מידע ציבורי?

מאת עו"ד יהונתן קלינגר

הקדמה

לאחרונה פסק בית המשפט העליון (כב' השופטת ענת ברון) כי חברת ביטס אוף גולד, חלפן ביטקוין מתל-אביב, יוכל להמשיך לנהל את עסקיו בבנק לאומי במשך הערעור שהגיש כנגד בנק לאומי (עא 6389/17 ביטס אוף גולד נ' בנק לאומי). ערעור זה הוגש לאחר שבחודש יוני 2017 פסק בית המשפט המחוזי (תא 1992-06-15 ביטס אוף גולד נ' בנק לאומי) כי הבחירה של בנק לאומי לסרב לנהל חשבון עבור חלפן ביטקוין הוא סביר במסגרת מערכת ניהול הסיכונים של הבנק. הסירוב של בנק לאומי עבור ביטס אוף גולד אינו בודד במערכה; בחודשים האחרונים בנקים ישראלים חוסמים ניהול חשבונות או קבלת העברות של לקוחות הקשורים למטבעות דיגיטליים בכלל. הטענה הכללית של אותם בנקים היא כי מדובר בניהול סיכונים רלוונטי למניעת הלבנת הון.

אלא, שהכרה של הטכנולוגיה לעומק מצביעה על כך שלא רק שמדובר על טענה שגויה בבסיסה, אלא כי ברוב המקרים השימוש במטבעות אלו מספק לבנקים מידע טוב יותר מאשר מזומן, ולעיתים גם מאשר העברות בנקאיות. לצורך כך, נציג מספר דרכים למניעה, התמודדות וניתוח של תשלומים על הרשת, ולאחר מכן נציג גם כיצד ניתן למזער נזקים אפשריים.

נזכיר, מה זה ביטקוין (מאמר שלי באתר כתב העת "משפט ועסקים"). ב-2008 מפרסם "סטושי נקמוטו" (שם עט) מאמר בו הוא מציע שיטת תשלומים אלקטרונית מבוזרת. הצעתו של נקמוטו מבוססת על שתי טכנולוגיות שהיו קיימות באותה העת: חתימה אלקטרונית (כלומר הצפנה) ושיתוף קבצים. הרעיון של נקמוטו היה כי יוקם מאגר מידע מבוזר, שמאוחסן על מחשבים רבים, ואשר יתעדכן בכל עשר דקות. כל עדכון כזה נקרא "בלוק" ובמהלך העדכון (בהפשטה יתרה) ידווחו כל אחד מהמחשבים המחוברים לרשת על העסקאות שעברו דרכו. כדי לוודא כי אף אחד מהמחשבים לא משנה בלוק עבר, לכל בלוק תהיה חתימה אלקטרונית בסופו, ויכיל גם את החתימה של הבלוק שלפניו. בכך, תווצר "שרשרת בלוקים" (blockchain) שמאפשרת לוודא כי לא בוצעו כל שינויים במערכת המידע.

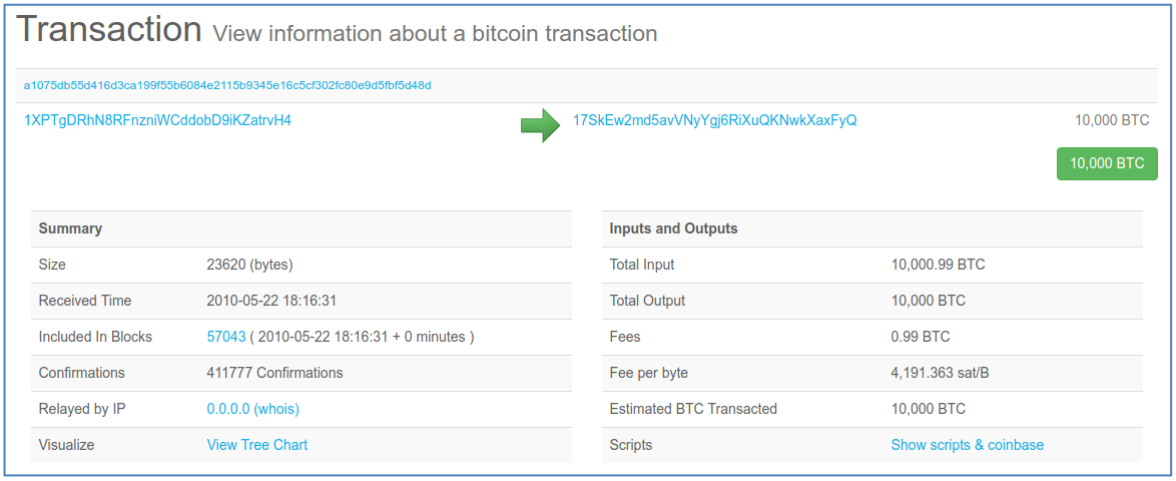
מדוע כך הדבר? אם לצורך העניין אני הצלחתי להשתלט על כל המחשבים ברשת ולשנות עסקה שבוצעה לפני שני בלוקים, הרי שכל החתימות האלקטרוניות יהיו שונות, ולכן תהיה שגיאה בשרשרת הבלוקים.

כיצד נוצר כסף חדש, אם כן? נקמוטו הציע כי בסיומו של כל בלוק יחולק גמול של 50 מטבעות אשר יועבר למי שהצליח לנחש את החתימה של הבלוק, כלומר מי שהפעיל כח מחשוב. הגמול הזה דועך לאורך זמן (כיום הוא על 12.5 מטבעות) ועד לשנת 2140 צפוי להעלם כלל. כך, נוצרים מטבעות על ידי כריה של בלוקים בשרשרת.

הרעיון העיקרי מאחורי ביטקוין הוא כי מדובר על מאגר מידע ציבורי, המכיל פרטים רבים. באמצעות התקנה של תוכנת ביטקוין על המחשב ניתן לא רק לקבל עותק של כל מאגר המידע, אלא להמשיך ולשתף את המידע עם כולם, בדיוק כמו תוכנת שיתוף קבצים. ישנן דרכים לעיין באותו מאגר. כלומר, אם אני משלם עבור קפה בבית קפה, הרי שהעסקה תוצג בשרשרת הבלוקים.

האנונימיות של ביטקוין .ביטקוין, לכשעצמו, אינו אנונימי אלא פסבדונימי. כלומר, לכל משתמש יש כתובת (או מספר כתובות) אשר העסקאות נחתמות על ידה. שמו של המשתמש אינו מופיע לצדו, וגם לא פרטי זיהוי אחרים, וכל שדרוש על מנת להשתמש בכתובת זו הוא המפתח הפרטי (שקול, בהפשטה יתרה במיוחד, לסיסמא) של המשתמש. אלא, שביטקוין כלל אינו אנונימי. כפי שראינו במקרים אחרים, ניתן להשתמש במידע ציבורי אנונימי ולהפוך אותו למידע מזוהה. הדוגמא של רב-קו ברורה לכולם: כיוון שיש רק אדם אחד שנוסע באוטובוס בימי חול בשעה 7:45 מתחנה ברח' קינג ג'ורג' בתל-אביב ושב בשעה 16:45 מתחנה שנמצאת ברח' ז'בוטינסקי 7 ברמת גן, וכיוון שיש רק אדם אחד שנוסע באוטובוס בימי ג' למשחקי כדורסל של מכבי תל-אביב מאותה תחנה ברח' קינג ג'ורג' למגרש ביד-אליהו, הרי שכל מה שצריך כדי לזהות את אותו אדם זה להמצא בתחנה ביום ושעה.

אותו דבר בדיוק עם כתובות ביטקוין. עצם זה שלצד כתובת ביטקוין אין את שמו של אדם, לא אומר שלא ניתן לזהותו. לדוגמא, נקח את העסקה הבאה מהבלוקצ'יין:


Transaction View information about a bitcoin transaction

a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

1XPTgDRhN8RFnzniWCddobD9iKZatrvH4 → 17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ 10,000 BTC

10,000 BTC

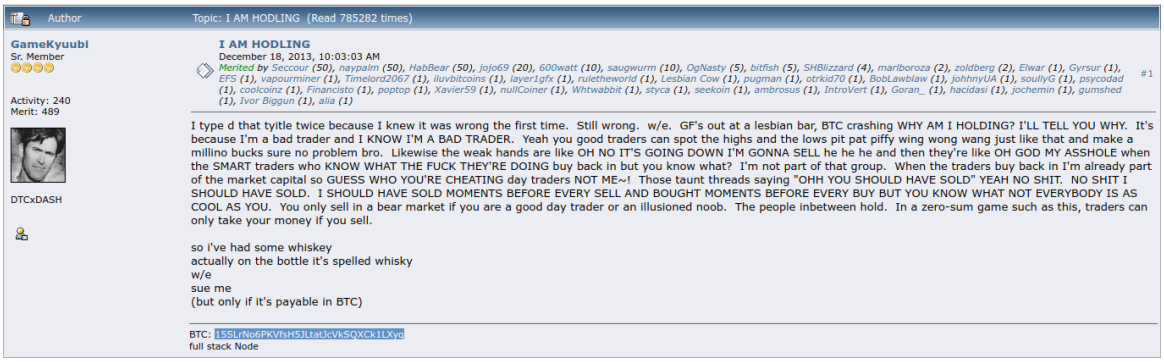
Summary	
Size	23620 (bytes)
Received Time	2010-05-22 18:16:31
Included In Blocks	57043 (2010-05-22 18:16:31 + 0 minutes)
Confirmations	411777 Confirmations
Relayed by IP	0.0.0.0 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	10,000.99 BTC
Total Output	10,000 BTC
Fees	0.99 BTC
Fee per byte	4,191.363 sat/B
Estimated BTC Transacted	10,000 BTC
Scripts	Show scripts & coinbase

כאן ניתן לראות עסקה שבוצעה ב-22 במאי 2010 ובה שולמו 10,000 מטבעות. בעסקה זו נרכשה הפיצה המפורסמת בשנת 2010, והיא ככל הנראה עסקת הביטקוין המתועדת הראשונה. יש בעסקה שתי כתובות: של האדם המשלם, ושל המקבל. כאשר לוחצים על כתובתו של כל אחד מהם, ניתן לראות מאלו כתובות התקבלו הכספים ולאן אותם כספים המשיכו לאחר מכן. אכן, לא לכל כתובת מוצמד "שם" של אדם, אבל הרבה מהכתובות יכולות להיות מזוהות.

זיהוי כתובות ביטקוין, חלק א'

בשלב הראשון, ניתן לזהות כתובות ביטקוין על ידי חיפוש ברשת. לדוגמא, כתובת הביטקוין 3HcEB6bi4TFPdvk31Pwz77DwAzfAZz2fMn היא כתובת של אתר שיתוף הקבצים The Pirate Bay. כלומר, ניתן להניח שאם אדם מסוים קיבל כספים מאותה הכתובת, הרי שהוא קשור בצורה כלשהיא לאתר, בין אם כנותן שירותים ובין אם כבעלים. לא רק אתרי שיתוף קבצים מפרסמים את כתובותיהם, גם משתמשים רבים בפורומים. לדוגמא, בפורומים של פיתוח תוכנה, נהוג לפרסם ככתובת לתרומה את כתובת הביטקוין. לדוגמא, בשרשור המפורסם הזה של פורום Bitcointalk ניתן לראות כי המשתמש שפרסם את ההודעה חתם עליה עם כתובתו:



כלומר, בשלב הראשון והמקדמי ביותר, ניתן לאתר האם כתובת מסוימת היא חשודה על ידי חיפוש שלה ברשת במקורות גלויים. הדוגמא הטובה ביותר היא מענה לשאלה "האם מקור הכספים הוא בפעילות הקשורה לנסיונות סחיטה ותוכנות כופר". תוכנות כופר הן, כידוע, תוכנות המצפינות קבצים על המחשב ואשר מתחייבות לשחררם רק לאחר תשלום. כדי להגן על הפושעים, הם משתמשים בתשלום שהם סוברים כי הוא אנונימי, ביטקוין. אלא שמרגע שכתובות אלו מפורסמות, הרי שניתן להניח שכל תשלום שבוצע מאותן כתובות הוא תשלום שמקורו בפשע זה. אתרים רבים מפרסמים את כתובות אלו למען הציבור, כך שניתן לאתרן בקלות יחסית.

כלומר, בשלב הראשון, ניתן להפחית כמות משמעותית של סיכונים על ידי איתור וניטור של מקורות גלויים המכילים כתובות שעשויות להיות חשודות.

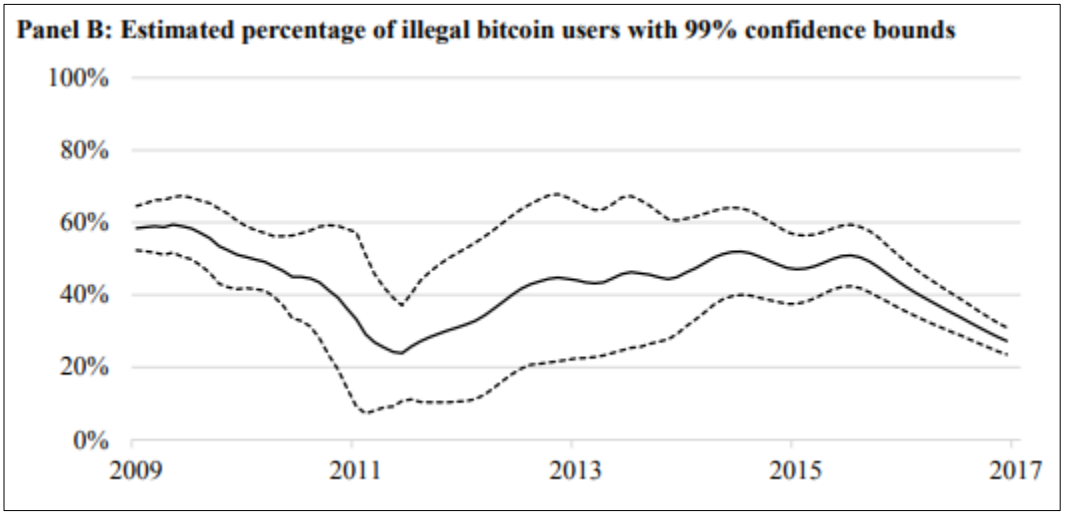
זיהוי כתובות ביטקוין למתקדמים, חלק ב'

אכן, כיוון שכל כתובות אלו מזוהות, הומצאו בשלב הראשוני של המטבע "מיקסרים". אותם מיקסרים בעצם מערבלים עסקאות. דמיינו מצב שארבעה אנשים רוצים לעשות שתי עסקאות שונות: א' רוצה לשלם לב' 100 ש"ח, וג' רוצה לשלם לד' 100 ש"ח. כדי לערבל את הכספים ולמנוע ודאות כי אכן א' שילם לב', אותם מיקסרים מקבלים מא' וב' 200 ש"ח ומשלמים לג' ולד' 200 ש"ח. אלא, שעצם השימוש במיקסרים הוא עסקה חשודה, שצריכה להדליק נורות. בפועל, עוד משנת 2013 הראו מחקרים כיצד ניתן לא רק לזהות מיקסרים כאלה, אלא גם כיצד ניתן לנתח אחורה בהסתברות סטטיסטית האם הכסף מקורו בפעילות עבריינית.

גם מאמר של עדי שמיר ודורית רון הראה מידע דומה. שמיר ורון הניחו כי אם יש עסקה בה יש מספר גורמים המשלמים יחדיו, הרי שיש זהות בין הארנקים. לכן, באמצעות ניתוח סטטיסטי, ניתן היה לוודא (או לנחש) כי שתי כתובות שהיו חלק מאותה עסקה הן אותה כתובת.

בצורה כזו, אם עסקה מסוימת עברה דרך מיקסר או שמקורה בפעילות עבריינית, הרי שניתן בצורה קלה, אלגוריתמית, לסרב לבצעה או לדווח עליה לרשות המוסמכת.

זיהוי כתובות ביטקוין לעבריינים, חלק ג'. אכן, קיים חשש כי העדר פיקוח מרכזי על כספים יוביל לשימושים עבריינים. החשש הזה קיים מצדן של רשויות אכיפה ושל בנקים; אך האם חשש זה מומש? מצד אחד, מאמר של חברת Eliptic מציג כי פחות מאחוז אחד מכלל המטבעות חלף בשלב כלשהוא דרך אתרי רשת אפלה והימורים, ומנגד מאמר אחר מדבר על כ-6% מכלל הארנקים ככאלה הקשורים לפעילות ברשת האפלה, וכ-25% מכלל העסקאות ברשת הקשורה לאותם ארנקים. אלא, שבשני המקרים, גם זה המספק מספר גבוה של עסקאות וגם זה המספק מספר נמוך, ניתן לראות כי כלל העסקאות החשודות אותרו. מעבר לכך, המאמר המציג כי 25% מהעסקאות קשורות לפעילות עבריינית מציג כי קיים טרנד של ירידה באחוז העסקאות העבריניות לאורך השנים:



אבל נמשיך. **בפועל, אין מניעה לזהות פעילות חשודה הקשורה לתחום הביטקוין**. כלומר, עוד לפני שנעבור לשימוש בכלים טכנולוגיים מתקדמים הקיימים כיום, חלפני ביטקוין יכולים להשתמש בטכנולוגיות ציבוריות על מנת לאתר פעילות חשודה; הם יכולים לאתר האם ארנק הביטקוין אליו מעוניין האדם הרוכש ביטקוין (או ממנו האדם הפודה מטבעות) מעורב בצורה כלשהיא באתרים חשודים, וזאת על ידי בדיקה ציבורית של הכתובות. עצם הבדיקה הראשונית הזו, של האם הכתובת עצמה קשורה לפעילות עבריינית (כלומר, האם העסקאות שבוצעו בעבר על ידי אותה כתובת היו לגורמים הידועים כעבריינים) יכולה למנוע חלק משמעותי של הלבנת הון.

בדיקה כפולה, כלומר שבה משתרשרת הבדיקה שני צעדים קדימה (האם האדם ששילם לאדם הנמצא מולי קשור לעסקאות עבריניות) יכולה להרחיב את ההגנה.

אבל לא בכך נשלם הדיון. הרי, יאמרו האנשים שרוצים להפחית את הסיכון, יבוא אלייך אדם נטול ארנק, ויפתח ארנק חדש וממנו יבצע פעילות עבריינית. אלא, שבשלב הזה אותם חלפני ביטקוין מבצעים פעילות של "הכרת הלקוח" כמו כל נותן שירותים פיננסיים. כלומר, לכל אחד מחלפני הביטקוין יהיה מידע לגבי (1) זהות המפקידים אצלהם; ו-(2) היקף ההפקדות שלהם. בהנחה שאותו ארנק בעתיד ישמש לפעילות עבריינית, הרי שהם יוכלו לדווח בצורה פרו-אקטיבית על כך לרשויות הרלוונטיות.

רשויות שיאתרו בעתיד פעילות עבריינית יכולו לפנות לחלפן הרלוונטי ולשאול אותו "האם כתובת X מוכרת לך?". ואיך ידעו מיהו החלפן הרלוונטי? ובכן, לכל חלפן כאמור יש כתובת. אם יזהו כי פעילות עבריינית מסוימת מקורה בכסף שהגיע מחלפן X, הרי שיוכלו לפנות אליו ולבקש את פרטיו של האדם שרכש מטבעות ממנו לכתובת זו.

כלומר, בפועל, להבדיל ממזומן, ובהנחה שחלפני הביטקוין מחזיקים מדיניות מניעת הלבנת הון טובה, השימוש במאגר מידע ציבורי שזמין גם למשתמשיו וגם לרשויות אכיפת חוק מאפשר מידע טוב יותר על העסקאות ואיתור אחורה של העסקאות. או ליתר דיוק, צריך להיות עבריין מטומטם במיוחד כדי להשתמש בביטקוין.

מאמר זה פורסם במקור כפוסט בבלוג "Intellect or Insanity" של עו"ד יהונתן קלינגר.