המחלקה הכלכלית

הרשות לניירות ערך

נייר עבודה

מטבעות דיגיטליים - סקירה ראשונית

ביטקוין כמקרה בוחן

ניקי קוצנקו, ד"ר גתית גור גרשגורן

אוגוסט 2014

נייר זה מהווה חלק מעבודת הרקע במסגרת צוות העבודה הבין-משרדי בנושא מטבעות דיגיטליים (כדוגמת ביטקוין).

הדעות המובאות בעבודה זו אינן משקפות בהכרח את עמדתה של רשות ניירות ערך.

תוכן עניינים

מטבעות דיגיטליים

מבוא

עלייתו של הביטקוין (Bitcoin) מאז תחילת הפצתו ב-2009 ובייחוד מאז תחילת שנת 2013 מחדדת את הצורך לבחינה מעמיקה של נושא המטבעות הדיגיטליים, לרבות השפעותיו האפשריות על ציבור המשקיעים ועל שוק ההון בישראל. בפברואר 2014 יצאה הודעה משותפת לרגולטורים בישראל שעוסקת במטבעות הדיגיטליים ובסכנות הכרוכים בשימוש בהם, באחזקתם ובהשקעה בהם. ההזהרה התמקדה בסכנות הנובעות מהמעמד החוקי והרגולטורי המעורפל של מטבעות דיגיטליים; מכך שאינם מהווים הילך חוקי[1] במדינה כלשהי; מהאפשרות לעשות בהם שימוש לצורך הלבנת הון[2]; ומפעילויות לא חוקיות נוספות שנעשות באמצעותם או בהקשר אליהם. כמו כן, ההזהרה הציפה סכנות נוספות שנובעות מהתנודתיות בערכם של המטבעות עצמם, מהקושי לשמור על המטבעות הדיגיטליים מפני גניבה, ומחוסר היציבות ומהפיקוח הרופף על אתרים ושירותי מסחר וחלפנות המטפלים במטבעות דיגיטליים. יחד עם זאת, נושא המטבעות הדיגיטליים נמצא עדיין בחיתוליו, הן מבחינת תפוצת השימוש במטבעות דיגיטליים, הן מבחינת המשך התפתחותם הטכנולוגית והן מבחינת הסדרה משפטית ורגולטורית של השימוש בהם. על כן, נדרשת למידה מתמשכת של הנושא על מנת להפיק תובנות לגבי היחס הנדרש כלפי הנושא בקרב מפקחים, מפוקחים והציבור הרחב.

צורך זה מתחדד לאור המגמות בתחום בתקופה האחרונה. מחד, שנת 2013 ראתה נסיקה חדה בערך המטבעות ובתפוצתם. ההערכות העדכניות הן של כ-63 אלף עסקים ברחבי העולם המקבלים ביטקוין כתשלום עבור השירות והמוצרים אותם הם מספקים.[3] חלק גדול מבתי עסק אלו אף מספקים מוצרים ברי

[1] הילך חוקי הוא אמצעי תשלום המשמש לתשלום חוב (לרוב חוב הנובע מעסקאות קניה או מכירה), אשר לא ניתן לסרב, על פי דין, לקבלו. מקור: ויקיפדיה.

[2] הלבנת הון היא פעולה פיננסית הנעשית תוך הסתרת זהות המקור והיעד של הכסף המועבר בפעולה זו. בדרך זו ניתן להפוך "הון שחור", שהוא כסף שמקורו בהשתמטות ממס או בפעילות פלילית (כגון סחר בסמים) לכסף שאינו מעורר חשד. הלבנת הון נחשבת לעבירה פלילית. מקור: ויקיפדיה.

[3] http://links.services.disqus.com/api/click?format=go&key=cfdfcf52dffd0a702a61bad27507376d&loc=http%3A%2F%2Fwww.coindesk.com%2Fstate-of-bitcoin-q2-2014-report-expanding-bitcoin-economy%2F&subId=2304995&v=1&libid=3e591679-b001-4437-bb31-7d1a1f0b2a38&out=http%3A%2F%2Fmedia.coindesk.com%2Freport%2FCoinDesk-State-of-Bitcoin-Q2-2014.pdf&ref=http%3A%2F%2Fwww.google.co.il%2Furl%3Furl%3Dhttp%3A%2F%2Fwww.coindesk.com%2Fstate-of-bitcoin-q2-2014-report-expanding-bitcoin-

קיימא שגרתיים, לדוגמא החנות האינטרנטית הגדולה Overstock.com המתמחה בבגדים, רהיטים, אלקטרוניקה ועוד מגוון מוצרים. ענקית המחשבים Dell החלה לקבל תשלומים בביטקוין ואף נותנת הנחה של 10% למבצעים רכישה באמצעות ביטקוין. [4] בנוסף, שלוש חברות גדולות (עם הכנסות של מעל 2 מיליארד דולר לשנה) נוספות החלו לאפשר רכישה באמצעות ביטקוין: חברת שירות הטלוויזיה בלוויין DISH, חברת שירותי התיירות Expedia, וחברת קמעונאות האלקטרוניקה Newegg. כמו כן, ניתן להשתמש בביטקוין על מנת לרכוש כרטיסי טיסה מחברות כגון צ'יפ אייר (cheapair.com) ואיר באלטיק[5] (AirBaltic), את שירותיהם של עורכי דין וסוכני נדל"ן, ולרכוש מגוון רחב של מוצרים ושירותים נוספים. נראה כי צרכנים אכן עושים שימוש באפשרות החדשה לשלם באמצעות ביטקוין: Overstock ו-Cheapair, הודיעו ביולי 2014 כי מכרו מוצרים בשווי של מעל 1.5 מיליון דולר כל אחת באמצעות תשלומים בביטקוין.[6]

יחד עם זאת, נראה שעיקר ההתעניינות בביטקוין עד כה הייתה כהשקעה. זאת, בעקבות זינוק בערך שלו במהלך שנת 2013 מערך כולל (סה"כ ביטקוין במחזור כפול מחיר דולרי של ביטקוין אחד) של כמעט 144 מיליון דולר (143,848,307) דולר במחיר של 13 דולר ל-1 ביטקוין בראשון בינואר 2013 לערך כולל של כמעט 14 וחצי מיליארד דולר (14,464,698,057) במחיר של 1203 דולר ל-1 ביטקוין ב-30 לנובמבר 2013, קפיצה של פי 100 בערך הכולל.[7] מאידך, בשלושת החודשים האחרים ערך הביטקוין נפל באופן חד וערכו עומד כעת (11.5.2014) על 443 דולר.

מגמות משמעותיות וסותרות אלה מבהירות את הצורך בסקירה ראשונית של ההיבטים המרכזיים הכרוכים בנושא המטבעות הדיגיטליים, סקירה שמסמך זה נועד לספק.

מהו מטבע דיגיטלי?

בשיח כיום בנושא, המושגים "מטבע דיגיטלי" ו"מטבע וירטואלי" משמשים באופן תחליפי. בעבודה זו נעדיף את המושג "מטבע דיגיטלי", כפי שמקובל בספרות המחקרית הראשונית שכבר מתהווה בתחום[8] ועל מנת שלא להטעות את הקורא לחשוב שהאופי הממוחשב של הביטקוין ודומיו הופך אותם באופן כלשהו ל"לא אמתיים", כפי שהמושג "וירטואלי" עשוי לרמז. מונח מקובל נוסף הוא מטבעות אלטרנטיביים (Alternative Currencies) או בקיצור אלטים (alts).

הבנק האירופי המרכזי (ECB), פרסם נייר עבודה באוקטובר 2012 בנושא מטבעות וירטואליים, העוסק במידה רבה בביטקוין. מטבע וירטואלי הוגדר בעבודה זו כסוג של כסף דיגיטלי, בלתי מפוקח, המונפק ונשלט על ידי מפתחיו, אשר נעשה בו שימוש בקרב המשתמשים של קהילה וירטואלית ספציפית[9].

---

economy%2F%26rct%3Dj%26frm%3D1%26q%3D%26esrc%3Ds%26sa%3DU%26ei%3DcjveU-7YEaic0AX_toDgAQ%26ved%3D0CBIQFjAA%26usg%3DAFQjCNGdfC4pM8I91x3d-bEFM5GdxcqrAw&title=State%20of%20Bitcoin%20Q2%202014%20Report%20Reveals%20Expanding%20Bitcoin%20Economy%20%23BTCreport2014&txt=%3CEM%3EDownload%20the%20full%20report%20in%20PDF%20form%3C%2FEM%3E&jsonp=vglnk_jsonp_14070731530661

[4] http://www.coindesk.com/dell-bitcoin-aligns-brand-innovation/

[5] http://www.coindesk.com/airbaltic-waives-controversial-bitcoin-transaction-fee/

[6] http://www.coindesk.com/cheapair-tops-1-5-million-in-total-bitcoin-sales/

[7] http://blockchain.info/charts/market-cap

[8] http://mercatus.org/publication/bitcoin-primer-policymakers

[9] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

נדמה שהמטבעות הדיגיטליים הצוברים תאוצה בשנה האחרונה חורגים מחלק מהגדרות אלה. הביטקוין למשל חורג מהן גם משום שקיימים סימנים של רגולציה מתהווה במספר מדינות בעולם (דיון מפורט על כך בהמשך), אולם בעיקר משום שהשימוש בו כיום אינו מוגבל לקהילה וירטואלית ספציפית אלא הולך ומופץ בקרב הציבור הרחב ברחבי העולם. בנוסף, יתכן שבזכות המודל המבוזר של הביטקוין (עוד על כך בהמשך), לא מדויק לומר שהוא נשלט על ידי מפתחיו, ויותר מדויק לומר שהוא נשלט במשותף על ידי קהילה אינטרנטית של "כורים" ועל ידי אלגוריתם ייצור שקובע את היצע הביטקוין. כמו כן, הקוד הפתוח שלו מאפשר לכל אדם לפתח אפליקציות ולהציע שינויים לקוד שלו באופן חופשי. נראה שהמטבעות הדיגיטליים המרכזיים שמתחרים בביטקוין כגון לייטקוין (Litecoin) ופירקוין (Peercoin), המתבססים על מודלים דומים לזה של הביטקוין, מאתגרים את ההגדרה הנ"ל באופן דומה.

באותה עבודה מקוטלגים סוגי המטבעות הווירטואליים ל-3 קטגוריות לפי כיווני הזרימה של החליפין:

1. סוג א' - רשת סגורה: המטבעות נצברים במסגרת אותה רשת שבה נעשה בהם שימוש. אין אפשרות להמיר מטבעות מדינתיים (כגון דולר) למטבעות אלה ולא להפך.
2. סוג ב' – זרימה חד-כיוונית: ניתן להמיר מטבע מדינתי במטבע וירטואלי מסוג זה, אבל לא ניתן להמיר חזרה.
3. סוג ג' – זרימה דו-כיוונית: ניתן להמיר מטבעות וירטואליים למדינתיים וחזרה.

לצרכינו העניין נסוב סביב סוג ג', אותם מקובל כיום לכנות "מטבעות דיגיטליים".

כמו כן, ישנה הבחנה בין כסף דיגיטלי לכסף אלקטרוני: כסף אלקטרוני (ערך כספי המאוחסן באופן אלקטרוני) שונה מכסף דיגיטלי בעיקר בכך שהוא נקוב באותו סוג מטבע כמו כסף פיזי, למשל דולרים. לעומת זאת, כסף דיגיטלי נקוב בסוג מטבע אחר, למשל ביטקוין. הבדל זה הוא משמעותי משום ששינוי סוג המטבע מייצר תופעה של שער חליפין בעל ניידות מסוימת בין המטבע המדינתי (כמו דולר) למטבע הדיגיטלי (כמו ביטקוין), ומגביל את האפשרות להמיר את המטבע הדיגיטלי חזרה למטבע המדינתי.

דוגמאות למטבעות דיגיטליים

המטבעות הדיגיטליים הגדולים ביותר לפי ערך כולל (Market Cap)[10]:

Volume (24h)	Price	Market Cap	Name
$ 6,988,024	$ 446.61	$ 5,696,772,505	Bitcoin
$ 2,040,454	$ 10.50	$ 296,543,008	Litecoin
$ 27,789	$ 2.13	$ 45,566,478	Peercoin
$ 142,802	$ 0.005805	$ 43,998,338	Ripple
$ 429,148	$ 0.000464	$ 35,777,190	Dogecoin
$ 53,637	$ 0.030841	$ 30,840,659	Nxt
$ 92,673	$ 2.06	$ 17,993,468	Namecoin
$ 27,525	$ 29.62	$ 16,679,190	Mastercoin

[10] http://coinmarketcap.com/. Accesses 11.5.2014

DarkCoin	$ 11,749,630	$ 2.76	$ 754,372

כפי שניתן לראות, הבמה המרכזית שמקבל כרגע הביטקוין בתקשורת העולמית אומנם משקפת (וגם מתחזקת) את מעמדו בתור המטבע הדיגיטלי המוביל, אך התחרות בין המטבעות השונים היא אינטנסיבית והפער בין ביטקוין לבין מתחרים מובילים יכול להצטמצם באופן משמעותי לאור התנודתיות הגבוהה של שערי החליפין במטבעות דיגיטליים.

כמבוא לנושא המטבעות הדיגיטליים, עבודה זו תתמקד ראשית בביטקוין. זאת מהסיבות הבאות: ראשית, מדובר במוביל שוק, הן מבחינת כמות העסקות המתבצעות באמצעותו והן מבחינת כמות העסקים הסטנדרטיים[11] שמקבלים אותו. לכן, הסיכוי להשפעתו על ציבור המשקיעים בישראל כיום הוא הגדול ביותר; שנית, 9 מתוך 10 המטבעות המובילים שניתן לראות בטבלה לעיל מבוססים במידה רבה על ביטקוין מבחינה טכנולוגית ולכן ביטקוין מהווה מבוא חשוב להבנתם גם כן; שלישית, גורמים שונים כבר החלו לפתח רמות נוספות של פונקציונאליות על גבי פרוטוקול הביטקוין[12]; ורביעית, משום שקיימת כבר קהילה מבוססת ושיח מפותח אודות ביטקוין. חשוב לציין כי למרות העניין הרב שמעורר הביטקוין, השימוש בו כיום הוא מוגבל ועומד על כ-40 טרנסאקציות בדקה בממוצע ב-12 החודשים האחרונים[13].

[11] הכוונה כאן לעסקים שאינם עוסקים בביטקוין או במטבעות דיגיטליים אחרים, בין אם במסחר בהם, במכירה של מוצרים או שירותים הקשורים אליהם, כמו תוכנות וחומרה ייעודיים וכדומה.

[12] במושג "פרוטוקול הביטקוין" הכוונה היא לתוכנת מחשב שמאפשרת שימוש במטבעות דיגיטליים מסוג "ביטקוין". מידע נוסף על כך בפרק "מהו ביטקוין" בתת-הפרק "ביצוע תשלום". למידע נוסף לגבי רמות נוספות של פונקציונאליות, נא לגשת לפרק "שימושים במטבעות דיגיטליים" בתת-הפרק "פיתוחים נוספים על גבי פלטפורמת ביטקוין"

[13] Blockchain.info. Accessed 11.5.2014

מהו ביטקוין?

ביטקוין הוא רשת תשלום ומטבע דיגיטלי מבוזר[14] המבוסס על פרוטוקול קוד פתוח (open source)[15]. ביטקוין מתואר לעיתים כ- cryptocurrency משום שהוא עושה שימוש בקריפטוגרפיה[16] למטרות אבטחה. מאמר שפורסם על ידי הבנק הפדראלי של שיקגו הגדיר את הביטקוין כמטבע דיגיטלי מבוסס אמון (fiduciary digital currency). נתחיל מתיאור השיטה שבאמצעות יכול ביטקוין, כך לטענת רבים מהמשתמשים והפרשנים הכותבים אודותיו, לתפקד כמטבע, ללא שטרות או מטבעות פיזיים, ללא גורם מפקח ומנפיק מרכזי וללא שירותי צד שלישי להסדרת תשלומים.

היסטוריה ואידיאולוגיה

ביטקוין הוצג לראשונה בשנת 2009 על ידי מפתח בעל השם הבדוי סאטושי נאקאמוטו (Satoshi Nakamoto). המניעים של נאקאמוטו ליצירת הפרויקט ולהעברתו אינם ידועים במלואם. אולם, עדויות של אנשים שעבדו עמו ושל טקסטים שפרסם מצביעים על השפעותיה של אידיאולוגיה ליברטריאנית על נאקאמוטו, אידיאולוגיה המבקשת לבטל את השפעותיהם של ממשלות ובנקים מרכזיים על ערך הכסף[17]. מאפיין אחד של ביטקוין שנועד להגשים מטרה זו הוא הגבלה על כמות המטבעות שיכנסו למחזור.

כיום, ניתן לראות ב"קרן הביטקוין" (Bitcoin Foundation - עמותה אמריקנית שמתפקדת כגוף לובי עבור קהילת הביטקוין) את הגורם המרכזי בקהילת הביטקוין, לאחר ש-Nakamoto "הוריש" את הפרויקט לגאווין אנדרסון (Gavin Andersen), המדען הראשי של הקרן. נאקאמוטו עצמו הפסיק את מעורבותו בפרויקט[18]. יחד עם זאת, ניתן להניח שמפאת אופיו המבוזר של הפרויקט (רשת מבוזרת וקוד פתוח) ההשפעה של קרן הביטקוין על ביטקוין הינה מוגבלת. עיקר השפעה זו מבוססת על תפקידו המרכזי של אנדרסון בקבוצה המצומצמת של מפתחי הליבה של ביטקוין[19].

הקוד של תוכנת ביטקוין זמין באתר גיטהאב (github.com) וכל אדם יכול להציע לתרום קוד שהוא פיתוח לצורך שדרוג התוכנה. ניהול הגרסאות ועיקר הפיתוח מתבצעים על ידי מספר אנשים שמקבלים הכרעות בינם לבין עצמם לגבי השינויים שיבוצעו בקוד. מנהיגם הלא מוכרז הוא אותו גאווין אנדרסון מקרן הביטקוין. אולם, חשוב לסייג את האמירה האחרונה לגבי השפעתה של אותה קבוצה סגורה של מפתחים. שיטת הקוד הפתוח והמבנה המבוזר של הרשת פירושו שיכול להתרחש מצב שבו אדם כלשהו מחוץ לאותה קבוצה יציע גרסה אלטרנטיבית של ביטקוין שלא תהיה מקובלת על אותה קבוצה מצומצמת אך תתקבל

---

[14] הארכיטקטורה של רשת הביטקוין היא מדגם peer-to-peer : ארכיטקטורת רשת מבוזרת שבה הצמתים השונים ברשת (שנקראים peers ויכולים להיות משתמשים בודדים או מחשבים בודדים) מתפקדים גם כספקים וגם כצרכנים של משאבים.

[15] קוד פתוח משמש בעולם התוכנה לציון תוכנה שקוד המקור שלה פתוח ונגיש לכל מי שחפץ בו והוא חופשי לשימוש, לצפייה, לעריכת שינויים ולהפצה מחודשת לכל אחד ואחת. מקור : ויקיפדיה.

[16] קריפטוגרפיה היא ענף במתמטיקה ומדעי מחשב לעיסוק ומחקר בשיטות אבטחת מידע ותקשורת נתונים על רבדיהם השונים, בסביבה פתוחה הנגישה לצד שלישי. מקור : ויקיפדיה.

[17] http://www.nytimes.com/2013/12/15/sunday-review/the-bitcoin-ideology.html?_r=0

[18] http://www.coindesk.com/companies/bitcoin-foundation/

[19] http://motherboard.vice.com/blog/whos-building-bitcoin-an-inside-look-at-bitcoins-open-source-development

על ידי קהילת המשתמשים. במקרה זה, גרסה זו תהפוך דה פקטו לביטקוין משום שהמשתמשים יורידו את העדכון שמציע הגורם החיצוני ולא את זה שמציעה הקבוצה, ולמעשה יעברו להשתמש בו[20].

רשת התשלום (Payment network)

כאשר מתבצעת עסקה במזומן, כלומר באמצעות מטבעות או שטרות שאינם דיגיטליים, קל יחסית לוודא שהכסף עבר מהצד הקונה לצד המוכר. הצד המקבל יכול לדעת שקיבל לידיו שטרות ויש לו אפשרות לבדוק שהשטרות אינם מזויפים באמצעות סימנים מזהים כלשהם. במקרה של עסקה המתבצעת באופן ממוחשב, גורם שלישי הנהנה מאמון הצדדים, כמו בנק או חברת אשראי, מאשר את העברת הכספים. ביטקוין שואף לאפשר ביצוע עסקאות ללא מעורבות של גורם שלישי מרכזי וללא העברה של שטרות מיד ליד[21].

עסקה בביטקוין מתבצעת כאשר נותן הביטקוין (הקונה) משתמש באפליקציה ממוחשבת כדי לשדר מסר פומבי לקהילת הכורים (miners, הסבר על כך בהמשך) בדבר העברה של כמות מסוימת של ביטקוין מחשבונו לחשבון המקבל (המוכר). כעת, זהו תפקידה של קהילת הכורים לוודא שהביטקוין שמועברים לחשבון המקבל לא הועברו במקביל לחשבון נוסף. זוהי בעיה שנקראת העברה כפולה (double spending), והיא המכשול המרכזי העומד בפני ביצוע עסקאות באמצעי תשלום דיגיטליים ללא גורם שלישי הנהנה מאמון הצדדים. בעיה זו נובעת מהעובדה שבניגוד לאמצעי תשלום פיזיים, העברה של אמצעי תשלום דיגיטלי לגורם אחר לא מסירה את המידע אודות אמצעי התשלום ממחשבו של המעביר. זה מאפשר למעביר להעביר את אמצעי התשלום לגורם נוסף. ביטקוין משתמש בפרוטוקול ייחודי כדי למזער את הסיכוי שמצב זה יתרחש. פרוטוקול זה מסתמך על משתמשים מיוחדים הנקראים "כורים". משתמשים אלה מקצים מכוח המחשוב שעומד לרשותם על מנת להפעיל את תהליך הווידוא. הם מתוגמלים על כך באמצעות עמלות מהעסקאות ובאמצעות מטבעות חדשים שמונפקים. לתהליך הווידוא יש שני מרכיבים.

1. במרכיב הראשון, כורים מנסים ליצור בלוקים (blocks). בלוק הוא קובץ הכולל שני חלקים עיקריים:
   א. הוא כולל קבוצה של טרנסאקציות שעדיין לא נכללות באף בלוק קודם. כלומר, בלוק הוא תיעוד של עסקאות שהתבצעו ברשת. לכן אם נצרף את כל הבלוקים לשרשרת אחת, נקבל תיעוד של כל העסקאות שהתבצעות אי פעם ברשת.
   ב. בנוסף, בלוק כולל גם פתרון לבעיה מתמטית קשה[22]. כורה שמוצא פתרון יכול ליצור קובץ של טרנסאקציות ולהוסיף אותו לשרשרת הבלוקים (blockchain) – רשימה מאוחדת פומבית של כל הטרנסאקציות שאושרו עד כה. הבעיה המתמטית הקשה נועדה להבטיח שישנה עלות ליצירה של בלוקים לא תקינים[23].
2. המרכיב השני של התהליך הוא שכחלק מתהליך צירוף הבלוק לשרשרת הבלוקים, נדרש כל כורה לאשר את כל הבלוקים הקיימים בשרשרת שאליה הוא רוצה לצרף את הבלוק שלו. האישור כרוך

[20] http://motherboard.vice.com/blog/whos-building-bitcoin-an-inside-look-at-bitcoins-open-source-development

[21] http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf

[22] למידע נוסף ראה נספח 2: פונקציית הגיבוב (Hash Function)

[23] http://en.wikipedia.org/wiki/Proof-of-work_system

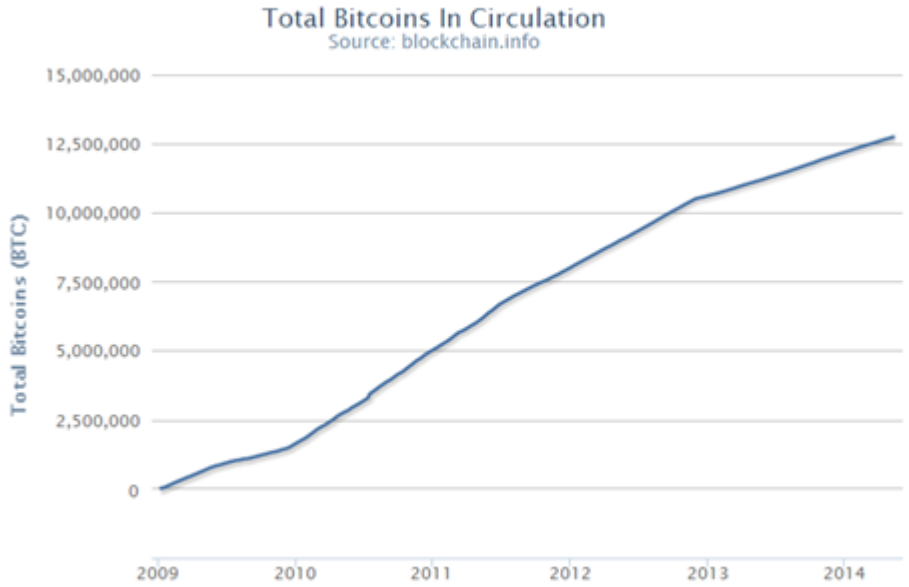
בבדיקה שכל הבלוקים בשרשרת תקינים. בלוק תקין הוא בלוק שלא כולל טרנסאקציות סותרות ושבו לכל ביטקוין יש היסטוריה תקינה[24].

למידע נוסף אודות הנחיצות של תהליך הווידוא ואודות מתקפות העברה כפולה ניתן לפנות לנספח 1: מתקפת העברה כפולה (Double Spending Attack).

הנפקה

הנפקת ביטקוין חדשים מתבצעת באמצעות מתן תגמול בביטקוין לכורה שפתר ראשון את הבעיה שאפשרה לצרף את קבוצת הטרנסאקציות החדשה (או הבלוק החדש) לרשימת הטרנסאקציות הקיימת[25]. גודלו של תגמול זה התחיל מ-50 ביטקוין ויורד בחצי כל 210,000 בלוקים (כל 4 שנים בערך, בהינתן קצב של 6 בלוקים לשעה). לפיכך סכום הביטקוין שיונפקו לעולם לא יעבור את ה-21 מיליון.[26]

התפתחות מספר המטבעות במחזור עד היום[27]:



[24] היסטוריה תקינה של ביטקוין היא שורת טרנסאקציות שמתחילה בהנפקה של ביטקוין לכורה, ממשיכה בשורה של טרנסאקציות תקינות (שנחתמו באמצעות המפתחות הפרטיים המתאימים למפתחות הפומביים של בעליהם) שבהן הביטקוין מועבר לבעלים הנוכחיים שלו, ומסתיימת בבקשת אותו בעלים להעביר את הביטקוין למישהו אחר.

[25] למעשה, כל מי שמצרף בלוק כלשהו, גם אם הבלוק ריק, מקבל את התגמול הנקוב. ניתן לנמק את ההיגיון שבמרכיב זה בשיטה במספר אופנים: ראשית, מורכבות הבעיה מושפעת באופן זניח בלבד מכמות הטרנסאקציות הכלולות בה ולכן כורים לא יעדיפו תמיד לצרף בלוקים ריקים. שנית, גם בלוק ריק מאשר את שרשרת הבלוקים הקיימת, כך שגם הוא תורם להבטחת אמינות השרשרת. שלישית, עמלות המחושבות לפי גודל העסקה מבטיחות שלכורה תמיד ישתלם יותר להוסיף את העסקאות שנושאות עמלה לבלוק שלו מאשר לצרף אותו ריק (זה כמובן כל עוד ישנן עסקאות הממתינות לאישור שכוללות עמלה).

[26] 2X50X210,000=21,000,000

[27] Accessed: 11.5.2014 ,Blockchain.info

כמות הביטקוין במחזור בטווח הקצר יכולה להיות מושפעת על ידי חוסר התאמה זמני בין רמת הקושי לאינטנסיביות של פעילויות הכרייה ולהיקף הטרנסאקציות שמתבצע, או כתוצאה מאובדן ביטקוין (בדרך כלל כתוצאה מאובדן קוד פרטי). משתנים אלה יכולים להביא לכך שסך הביטקוין במחזור בשלב שבו לא ניתן יהיה לייצר עוד ביטקוין יהיה נמוך מ-21 מיליון.

אחסון

על מנת לעשות שימוש בביטקוין אדם צריך להוריד אפליקציה הקרויה "ארנק ביטקוין" (Bitcoin wallet). אפליקציה זו מאפשרת את כל הפונקציונאליות של שימוש בסיסי בביטקוין. ראשית, היא מאפשרת הפקה של מפתחות. על מנת לעשות שימוש בביטקוין יש צורך בצמד מפתחות – מפתח פרטי ומפתח פומבי. המפתח הפומבי הוא למעשה כתובת הביטקוין של האדם שאליה הוא מקבל וממנה הוא שולח ביטקוין. הבעלות על ביטקוין משויכת למפתחות פומביים. לכל מפתח פומבי יש מפתח פרטי משלו ומפתח זה מתפקד כחתימה אלקטרונית ייחודית. על מנת לשלוח ביטקוין ממפתח פומבי מסוים, נדרשת חתימה של המפתח הפרטי התואם.

שליחת ביטקוין היא כאמור בקשה לעדכן את הרשת שכמות מסוימת של ביטקוין שייכת כעת למפתח פומבי אחר. לכן, הארנק לא מאכסן למעשה את הביטקוין שנמצאים בבעלות המשתמש. הארנק מאכסן את המפתח הפרטי של המשתמש ומאפשר לו לבצע פעולות כמו גישה פשוטה לשרשרת הבלוקים על מנת לדעת את היתרה שלו, שליחה של ביטקוין וכו'.

גניבת ביטקוין מתבצעת כאשר נגנב המפתח הפרטי. במקרה כזה, הגנב יכול לשלוח את כל הביטקוין המשויכים למפתח הפומבי של הקורבן לחשבונו ואז לבזבז אותם בכל אופן שירצה. אירועי גניבה של ביטקוין הפכו בחודשים האחרונים לדבר המדווח באמצעי התקשורת חדשות לבקרים. נדמה כי אמצעי האבטחה של הביטקוין מתקשים להתמודד עם המאמצים הרבים המושקעים על ידי האקרים ברחבי העולם כדי לבצע שוד ביטקוין.

על מנת להתמודד עם בעיות אבטחה אלו, פותחו אמצעים לאכסן את המפתח הפרטי במקום שאליו אין גישה דרך הרשת. לשם כך קיימים ארנקי נייר וארנקי חומרה. ארנקים אלה לא מחליפים לחלוטין את ארנק התוכנה שרק דרכו ניתן לשלוח ביטקוין. ארנקי נייר מאפשרים אחסון של מפתח פרטי על דפים מודפסים כאשר נדרש ארנק תוכנה ייעודי שסורק את קוד הזיהוי המהיר (QR) המקדד את המפתח הפרטי מהדף המודפס לפני ביצוע של כל טרנסאקציה. ארנקי חומרה פועלים בצורה דומה, כאשר את הסריקה מחליף מנגנון גישה מאובטח אל ארנקי החומרה, המהווים התקן חיצוני שלא מאפשר גישה ישירה לאינטרנט.

פומביות ופסבדונימיות (Pseudonimity)

כאשר שני אנשים מבצעים ביניהם עסקה מבלי שאף אחד מהם יחשוף את זהותו בפני השני ומבלי ששום גורם שלישי ידע על כך, נאמר שהעסקה ביניהם הייתה פרטית ואנונימית. כיום, מצב זה אפשרי רק בהחלפת כסף מזומן בין שני אנשים פרטיים. לעומת זאת, עסקאות המתבצעות באמצעות כרטיס אשראי הן פרטיות, במובן זה שרק שני הצדדים לעסקה וחברת האשראי יודעים על ביצוע העסקה אך הן לא אנונימיות, במובן זה שכל צד יודע את זהותו של הצד השני. זהו המקרה גם ברכישה באמצעות שירותי תשלום אינטרנטי כמו פייפאל (PayPal)[28].

[28] Paypal.com הוא נחשב בעיני רבים להיות שירות התשלום האינטרנטי הנפוץ בעולם

המקרה של ביטקוין הוא שונה. בביטקוין עצם קיומה של עסקה בגודל מסוים בתאריך כלשהו היא פומבית לחלוטין, משום שהיא מתועדת בשרשרת הבלוקים הנגישה לכל. אולם, העסקה נרשמת כהעברת ביטקוין בין שני מפתחות פומביים, כאשר הקשר בין המפתח הפומבי לזהות האדם שמחזיק במפתח הפרטי הקשור אליו יכול להישאר חסוי. כאמור, ארנקים מאפשרים שכל עסקה תתבצע באמצעות צמד חדש של מפתחות על מנת להקשות על זיהוי באמצעים סטטיסטיים. לכן מקובל לומר שעסקאות ביטקוין הן פומביות ופסבדונימיות. כלומר, הן נעשות לעיני כל, אך באמצעות מעין זהות בדויה.

יש הטוענים שמאפיין זה של הביטקוין הופך אותו לכלי יעיל להלבנת הון, אולם מומחים בנושא (ראה בהמשך דיון על יחס הרגולטורים בארה"ב לביטקוין) טוענים שמטבעות דיגיטליים מבוזרים הם פחות יעילים להלבנת הון מאשר מזומן. מתקיים כיום דיון תיאורטי ראשוני בקהילות המשתמשים במטבע הדיגיטלי ובקהילות הקריפטוגרפיה לגבי האפשרות לאתר את האדם מאחורי הקוד הפרטי. מספר עבודות אקדמיות עוסקות במגבלות האנונימיות של רשת הביטקוין וטוענות שניתן למעשה לאתר גם משתמשים השואפים להימנע מאיתור[30][29]. מנגד, קיימת הטענה שמשום שקיימים ארנקים המאפשר לייצר זוג מפתחות חדשים לכל טרנסאקציה, לא ניתן לגלות את זהותו של משתמש זהיר.

[29] http://anonymity-in-bitcoin.blogspot.co.il/2011/07/bitcoin-is-not-anonymous.html

[30] http://book.itep.ru/depository/bitcoin/User_privacy_in_bitcoin.pdf

שימושים במטבעות דיגיטליים

שימוש כמטבע

מטבע (Currency) הוא אמצעי חליפין – משהו שמתקבל בתמורה לשירות או מוצר על מנת לשמש במועד אחר לחליפין תמורת שירות או מוצר אחרים. מרבית המטבעות בעולם כיום הם מטבעות פיאט (Fiat Currency) – מטבעות שמקבלים את ערכם כתוצאה מהגדרתם על ידי המדינה בתור המטבע הרשמי במדינה וכתוצאה מהבטחה של המדינה לשמור על ערכם. מטבעות פיאט אינם מגובים על ידי המדינה, כלומר, לא ניתן להחליפם בכמות קבועה של סחורה בעלת ערך, כפי שהיה אפשרי בתקופת סטנדרט הזהב[31]. לפיכך, מקובל לומר שמטבעות אלה הם בעלי ערך בזכות האמון שהם ימשיכו להתקבל כאמצעי חליפין בעתיד, אמון שמבוסס על התחייבות הממשלה לשמור על ערך המטבע.

בנוגע למטבעות דיגיטליים, עולה השאלה אם הם כלל מתאימים להגדרה כלשהי של מטבע. מבחינה משפטית, עולה שמדינות רבות שומרות את ההגדרה של מטבע למה שהוכר במדינה כהילך חוקי[32] (מטבע מקומי) או שהוכר במדינה אחרת כהילך חוקי (מטבע חוץ). יחד עם זאת, מטבע דיגיטלי יכול להתאים להגדרה הכלכלית של מטבע שצוינה לעיל, כדבר מה שמשמש כאמצעי חליפין. במכתב של הבנק הפדרלי של שיקגו, אכן הוגדר ביטקוין כמטבע מבוסס אמון (Fiduciary Currency).[33] בדומה למטבעות פיאט גם ערכם של מרבית המטבעות הדיגיטליים (כגון ביטקוין) כמטבעות מבוסס על מערכת דומה של אמון, אך בשונה מהם, אמון זה מתקיים בין המשתמשים בלבד ולא מעורבת בו שום כפייה או התחייבות של ממשלה כלשהי.

הכלכלן ג'ורג' סלגין (George Selgin) הציע חלוקה אנליטית לארבע קטגוריות של משטרים מוניטריים, כאשר ביטקוין מהווה דוגמא לאחד מאותם משטרים. הוא מציע לאפיין כל סוג של מטבע/משטר מוניטרי לפי שני פרמטרים: ראשית, האם המחסור במטבע הוא מוחלט (טבעי או בלתי ניתן לשינוי), או מותנה (תלוי בהחלטות של ממשל, פרלמנט או גורמים בשוק התחרותי); שנית, האם למטבע יש שימוש לא מוניטרי, כלומר שימוש כאמצעי חליפין, בדומה למלח, או שאין לו שימוש לא מוניטרי, בדומה לשטרות.

		שימוש לא מוניטרי	
		יש	**אין**
מחסור	**מוחלט**	סחורה	סחורה סינתטית
	מותנה	Coase Durable	פיאט

סחורה – המלח כמטבע נמצא במחסור טבעי (לפחות היה כך בזמן הקדום שבו שימש כמטבע) וערכו נובע בחלקו משימוש לא מוניטרי. לפי סלגין, הבעיה עם מטבעות מהסוג הזה היא שהמחיר שלהם משתנה

[31] סטנדרט הזהב הוא מצב שהיה מקובל במרבית המדינות המפותחות ובוטל בהן בהדרגה במהלך המאה ה-20. זהו מצב שבו מי שמחזיק בשטר כסף יכול להגיע עם השטר לבנק המרכזי ולקבל תמורתו כמות כלשהי של זהב בהתאם לערך הנקוב על השטר.

[32] http://he.wikipedia.org/wiki/%D7%94%D7%99%D7%9C%D7%9A_%D7%97%D7%95%D7%A7%D7%99

[33] http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf

בטווח הארוך, ולעיתים באופן דרסטי. זה יכול להיגרם משינויים בהיצע, למשל כתוצאה מהתפתחות טכנולוגיית ההשגה שלהם, או משיניים בביקוש, למשל כתוצאה מגילוי שימושים לא מוניטריים נוספים.

פיאט – לשטר דולר אין שימוש לא מוניטרי והמחסור בו מותנה על ידי מדיניות הבנק המרכזי שיכולה להשתנות ולהרחיב את ההיצע שלו. לפי סלגין, לא משנה אצל מי נמצאת היכולת לקבוע את היצע הכסף, תמיד תהיה אסטרטגיה באמצעותה אותו גורם יוכל להרוויח מהגדלת ההיצע באופן שלא יעלה בקנה אחד עם האינטרסים של הכלכלה כולה. לפיכך, התוצאה המתבקשת היא קריסה בערך המטבע.

Coase Durable – כינוי של סלגין לסוג המטבע שהציע הכלכלן רונלד קואס (Ronald Coase). קואס מדגים מדוע מטבע שהמחסור שלו מותנה, גם אם יש לו שימוש מוניטרי, ערכו יקרוס באותו אופן כמו מטבע פיאט. כלומר, שימוש לא מוניטרי לא מונע קריסת ערך כל עוד המחסור מותנה.

סחורה סינתטית – לפי סלגין ביטקוין הוא סוג מטבע שבו לא קיימים אף אחד מהקשיים שצוינו לעיל. לא ניתן להרחיב את ההיצע שלו בהחלטה או כתוצאה משינוי טכנולוגי. כמו כן, אין לו שימוש לא מוניטרי ולכן הביקוש שלו ייקבע מגורמים מוניטריים בלבד. בנוסף לכך, הוא אינו מתבלה ומאפשר חלוקה עצמית כמעט אינסופית.[34] לשיטתו של סלגין, אחד היתרונות הבולטים של משטר מסוג כזה הוא היציבות, ואף העלייה בערך המטבע. מחד, המטבע מוגן בפני אינפלציה כתוצאה מהדפסת כסף ומאידך, ערכו עולה יחד עם העלייה בערכם של הסחורות אותם הוא קונה (כתוצאה מצמיחה כלכלית). יתרון נוסף של מטבעות וירטואליים המשתמע מטיעונו של סלגין נעוץ בכך שלשיטתו, מערכת ממוחשבת הפועלת באופן בלתי תלוי הינה ראויה יותר לאמון, בהקשר של שמירה על ערך המטבע, מאשר גורם אנושי.

אם כך, אפשר לסכם את היתרונות של השימוש בביטקוין כמטבע באופן הבא:

1. היצע קבוע המובטח על ידי מערכת אמינה ובלתי תלויה, מה שמסייע לשמור על ערך הביטקוין מפני שחיקה
2. היעדר ביקוש לא מוניטרי, מה שמסייע למנוע שינויים חדים בערך המטבע
3. אינו מתבלה
4. מאפשר חלוקה לשברירים בכל גודל
5. מאפשר לבצע עסקאות ללא ידיעתו של גורם שלישי את זהות הצדדים בעסקה (כפי שהוסבר לעיל, ניתן לדעת שכמות כלשהי של ביטקוין עברה מכתובת אחת לכתובת אחרת)

אולם, יתכן שאופטימיות זו של סלגין ושל גורמים נוספים, הרואים במטבעות דיגיטליים כדוגמת הביטקוין את התגלמות המשטר המוניטרי האידיאלי, הינה מוקדמת. ביטקוין עוד לא הפך לאמצעי תשלום מקובל מלבד בקרב קבוצה מצומצמת, אם כי גדלה והולכת, של סוחרים. כ-23,000 עסקים מקבלים ביטקוין, המהווים חלקיק אפסי מכלל העסקים הפועלים בעולם. מספר הטרנסאקציות היומי בביטקוין במהלך שנת 2013 עמד על כ-40 אלף, בעוד מספר הטרנסאקציות היומי בויזה[35] (Visa) באותה שנה היה 24 מיליון. מספר זה של טרנסאקציות בביטקוין נמצא במגמת עליה, אך לא ברור אם עלייה זו היא מגמה ארוכת טווח או אופנה חולפת.

ואכן, קיימים חסרונות ממשיים לשימוש בביטקוין כמטבע:

---

[34] http://tmtfree.hd.free.fr/albums/files/TMTisFree/Documents/Economy/Synthetic%20Commodity%20Money.pdf

[35] חברת אשראי ושירותים פיננסיים בינלאומית. למידע נוסף: www.visa.com

1. התנודתיות הרבה של הביטקוין פוגעת ביכולתו לשמש כשומר ערך, תכונה חשובה ביותר של מטבע. תנודתיות גדולה זו יוצרת עלויות סיכון כתוצאה מאחזקתו, שהופכת את אחזקתו ללא כדאית ביחס למטבעות אחרים. נראה שתנודתיות הביטקוין התגברה בשנה האחרונה. בעוד שבשנת 2013 שיעור השינוי היומי הממוצע של ערכו (בערך מוחלט) היה 4.5%, בחודש שבין 5/12/13 – 5/01/14 הממוצע היה 6.5%. בנובמבר 2013 השינוי היומי הממוצע אף הגיע ל-8.3%. בשנת 2013 היו 42 ימים שבהם השינוי היומי בערכו היה מעל 10%. סטיית התקן של מחירי הביטקוין ירדה בהדרגה מ-26 ברבעון הראשון ל-21 ברבעון השלישי רק כדי לקפוץ ל-330 ברבעון האחרון. פול קרוגמן במאמר בניו יורק טיימס טוען שמשום שאין ערך מינימאלי לביטקוין, יהיה קשה להסתמך עליו ככלי יעיל לשמירת ערך (store of value)[36]. אולם, ניתן לשער שככל שיתרחב השימוש בביטקוין כמטבע, הדבר יביא לירידה בתנודתיות שלו כתוצאה מעלייה בנזילות וחשיבותו של גורם מרתיע זה תפחת.
2. מטבעות דיגיטליים לא מהווים הילך חוקי בשום מדינה. היותו של מטבע הילך חוקי יוצר ביקוש יציב לאותו מטבע כתוצאה מהאפשרות לשלם באמצעותו מיסים וכתוצאה מחיובם של נושים לקבל את אותו מטבע למטרת פדיון חוב.
3. תועלות חיצוניות רשתיות (Network Externalities) של מטבעות מדינתיים, כלומר, העובדה שאנשים רבים כבר משתמשים בהם, מהווה יתרון משמעותי שלהם על פני המטבעות הדיגיטליים החדשים.
4. הנטייה הדיפלציונית של מטבעות דיגיטליים בעלי היצע מוגבל עלולה להוביל לאגירה של אותו מטבע דיגיטלי במקום להשתמש בו לביצוע עסקאות, דבר שיפגע בשימוש בו. פרד וילסון, ממקימי קרן ההון סיכון Union Square Ventures הציג בהרצאה ב-NYU כמה מהבעיות המרכזיות שמונעות לטענתו מהערך של ביטקוין לעלות. לטענתו אנשים שמחזיקים כרגע בביטקוין אוגרים אותו בציפייה שערכו יעלה, וכך יוצרים בעיות נזילות וגורמים לערכו לרדת.[37]
5. המורכבות הטכנולוגית של המטבעות הדיגיטליים גם היא עלולה להיות גורם מרתיע בפני אימוצם. המטבעות הללו מופעלים באמצעות מערכות ממוחשבות שאנשים רבים אינם מבינים ויתקשו לסמוך עליהן. בנוסף, מערכות אלה אינן נתונות כיום לפיקוח של שום גורם ממשלתי, מה שיכול לפגוע עוד יותר באמון שאזרחים מן השורה יתנו בהן.
6. פערי האבטחה בשירותי אכסון, חלפנות ומסחר של ביטקוין שהתגלו כתוצאה משורה של אירועי פריצה ממוחשבת וגניבה בשנה האחרונה גם הם פוגעים באטרקטיביות של השימוש בביטקוין כמטבע.

שימוש כמערכת תשלום

מההסבר על צורת הפעולה של ביטקוין ניתן לראות שלצד היותם של ביטקוין שנמצאים ברשותו של אדם מטבעות, קיימת מערכת המאפשרת ביצוע תשלומים בביטקוין. מערכת זו כוללת את רישום התשלום ושיטת וולידציה לכך שהתשלום עבר בהצלחה ואינו ניתן לביטול. אומנם לא ניתן להעביר ביטקוין לאדם אחר ללא שימוש באותה מערכת, אך ניתן להשתמש במערכת זו כמערכת תשלום, מבלי להחזיק ביטקוין כמטבע באופן קבוע. ניתן לחשוב על שירות שבו אדם משלם בדולרים שברשותו, הדולים מומרים

[36] http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/?_r=0

[37] /http://www.coindesk.com/investor-fred-wilson-security-hoarding-holding-back-bitcoin

אוטומטית לביטקוין, המועברים למוכר באמצעות מערכת הביטקוין, ושם מומרים חזרה לדולרים. כך קונה ומוכר, המשתמשים בדולרים בלבד, העבירו ביניהם תשלום על גבי מערכת הביטקוין. סוג שירות זה ניתן כבר על ידי מספר גורמים, ביניהם האתר ביטפיי (Bitpay), וחברות משמעותיות עושות בו שימוש, כדוגמת אתר הבלוגים מהגדולים בעולם וורדפרס (WordPress)[38].

דיון ראשוני מתקיים כיום לגבי היתרונות והחסרונות של השימוש במטבעות דיגיטליים כמערכות תשלומים. הסוגיות המרכזיות בדיון זה הן עלות השימוש, פרטיות, אפשרות לעקוף מגבלות על תנועות הון, ואפשרות לבטל עסקה לאחר ביצועה.

בנושא העלות קיימות טענות לכאן ולכאן. מחד, גורמים שונים טוענים שעלויות העסקה בביטקוין הינן נמוכות באופן משמעותי מאשר באמצעים מתחרים. למשל, שליחת כספים על ידי עובדים זרים חזרה למשפחותיהם בעולם השלישי הגיעה ל-400 מיליארד דולר בשנת 2012, ומחיר העברה ממוצע עמד על 9% מגובה ההעברה, לפי עיבוד של מכון מרקטוס (Mercatus) לנתוני הבנק העולמי. לפי עבודה של אותו מכון, הפועל במסגרת אוניברסיטת ג'ורג' מייסון (George Mason University), העברות מסוג זה יכולות להתבצע באמצעות מערכת ביטקוין עבור עד 1% מערך העסקה, כלומר חסכון של לפחות שמונה תשיעיות מהעלויות. כמו כן, אותה עבודה טוענת שעסקים קטנים המקבלים תשלום בביטקוין יצמצמו את עלויות העסקה הנגרמות להם על ידי חברות כרטיסי האשראי[39].

מנגד, מאט לוין (Matt Levine), בלוגר באתר בלומברג (Bloomberg) העלה את הטענה כי שיטת הכרייה של רשת הביטקוין נושאת בחובה את עיקר העלויות של ביצוע עסקה. לטענתו, רווחיהם של הכורים עומדים כיום על 3.5% מהיקף העסקאות בהן הם טיפלו[40]. כלומר, עלות העסקה הממוצעת בביטקוין אינה מסתכמת בתשלום הוולונטארי של עמלת עסקה שנועדה לעודד אישור מהיר לעסקה, אלא עומדת על 3.5%, שהם סך רווחי הכורים ביחס להיקף הטרנסאקציות בהן טיפלו. מחד ניתן לטעון שהגידול בהיקף הטרנסאקציות והירידה בתמורות הכרייה עם הזמן יכולות לגרום לאחוז זה לרדת. אך מנגד ניתן לטעון שכורים יצפו לקבל תגמול גדל והולך באמצעות עמלות וקשה להכריע מה יהיה תגמול הכורים בשיווי משקל.

בנוסף, בדוגמא שניתנה לעיל, שבה שירות מבצע המרה אוטומטית עבור שני צדדי העסקה, השירות חשוף לסכנת התנודתיות של ביטקוין. הנזילות המוגבלת של הביטקוין לא בהכרח תאפשר למפעיל השירות לפדות את הביטקוין במחיר שבו הוא קיבל אותם. לכן הוא יאלץ לגבות מלקוחותיו עמלות מוגדלות כדי לפצות אותו על הסיכון, וזה יכול להפוך את השירות ליקר יותר ממתחרים הפועלים באמצעות מטבעות מדינתיים.

סוגיה נוספת היא פרטיות, שזכתה כבר להתייחסות במסגרת הפרק על השיטה הפסבדונימית של הרשת. גם בהקשר זה ישנם טיעונים לשני הצדדים. מחד, המשתתפים בתשלום לא חושפים את פרטיהם באופן ישיר לגורם שלישי כמו חברת כרטיס האשראי או הבנק. מאידך, הם חושפים חלק מפרטי העסקה (כמה ביטקוין עברו מתי ובין אילו קודים פומביים) לעיני כל. חשיפה זו נעשית אומנם תחת ההגנה של כתובת ציבורית שזהות בעליה אינה ידועה, אך אם זהות זו נחשפת, פרטי העסקה יהיו ידועים מיד לכל מי שיחפוץ בכך.

[38] http://techliberation.com/2013/04/05/why-bitcoins-valuation-doesnt-really-matter/

[39] http://mercatus.org/publication/bitcoin-primer-policymakers

[40] http://www.bloomberg.com/news/2014-01-02/bitcoin-is-an-expensive-way-to-pay-for-stuff.html

יתרון נוסף שעומד כיום למטבעות דיגיטליים כמערכות תשלום, לפחות מנקודת המבט של גורמים מסוימים, הוא האפשרות להשתמש בהם כעקיפה של מגבלות על תנועות הון. אולם סביר להניח שאפשרות זו תהפוך ליותר ויותר מוגבלת ככל שהרגולציה על התחום תתהדק.

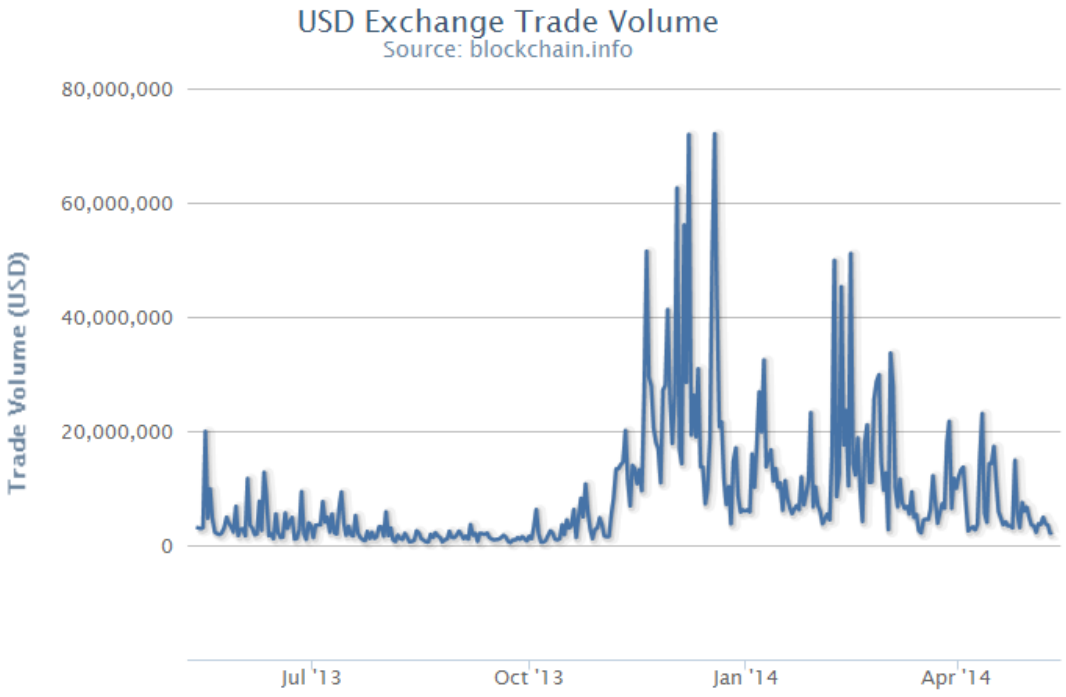
חסרון נוסף הוא שמערכת הביטקוין לא מאפשרת ביטול עסקה אחרי אישורה ולא תמיד אפשר לאתר את זהות המקבל, מה שמקל על הונאות כאשר ביטקוין הוא אמצעי התשלום.

שימוש כאפיק השקעה

לשם נוחות, נחלק את אפשרויות ההשקעה בביטקוין למספר קטגוריות: השקעה ישירה, השקעה עקיפה, והשקעה במניות באמצעות ביטקוין.

השקעה ישירה בביטקוין, כלומר, באמצעות רכישה ומכירה של המטבע הדיגיטלי עצמו, מתאפשרת באמצעות זירות מסחר אינטרנטיות. זירות אלה מאפשרות לקנות ולמכור ביטקוין ומטבעות דיגיטליים נוספים בעבור מטבעות מדינתיים כמו דולר ויורו וגם להחליף מטבעות דיגיטליים זה בזה לפי שערי חליפין המתבססים על העסקאות האחרונות שהתבצעו. דוגמאות בולטות לשירותים מסוג זה הן MtGox, BitInstant, Bitstamp, BTC China, BTC-E, Coinbase, Kraken (digital currency exchange).

סה"כ היקפי מסחר בפלטפורמות הגדולות (בדולרים)[41]:



[41] Blockchain.info, accessed: 11.5.2014

פלטפורמות המסחר הללו סובלות מחוסר יציבות, שלעיתים פוגעת קשות בציבור המשקיעים בהן. כמו כן, קיימים קשיים שונים בניהול תקין של המסחר בפלטפורמות וביניהן כתוצאה מבעיות אבטחה, בעיות טכנולוגיות והתערבויות רגולטוריות. למשל, ביום הבדיקה (05/01/2014) מרווחי קנייה-מכירה בפלטפורמות המרכזיות היו בסביבות ה-10 סנט. יחד עם זאת, נוצרו פערי ארביטראז' בין MtGox, אחת מפלטפורמת המסחר הגדולות בביטקוין, לבין המתחרים, בהיקף של כ-80 דולר (כ-9.5% מערך הביטקוין). עולה כי פער זה נבע מבעיות פדיון בדולרים ב-MtGox שגרם לירידה במחיר הדולר (ביחס לביטקוין) בפלטפורמה[42]. סיבה נוסף, כללית יותר, לפערי ארביטראז' המתקיימים בין הפלטפורמות השונות למסחר בביטקוין, היא עלויות העסקה הגבוהות בביצוע עסקאות בין הפלטפורמות[43]. כחודשיים לאחר מכן, במרץ 2014, הגישה חברת MtGox בקשה לפשיטת רגל בטענה שהיא הייתה קורבן של מתקפת האקרים נרחבת שהביאה לגניבה של מאות מיליוני דולרים בביטקוין. מנגד יש הטוענים כי מנהלי החברה משתמשים בגניבה כאמתלה ולמעשה הם אלה שאחראים לגניבת הכספים מלקוחותיהם[44].

בקרב פרשנים עולה טענה שנפילת MtGox כמו גם חוסר היציבות של האתר שקדמה לנפילה, הם מהגורמים להמשך הירידה בערך הביטקוין לאזור ה-400 דולר.

להלן גרף המדגים את תנודתיות המטבע ב-12 החודשים האחרונים[45]:

[42] http://bitcoin.stackexchange.com/questions/12670/why-dont-people-buy-at-one-exchange-and-sell-at-another

[43] https://bitcointalk.org/index.php?topic=212854.0

[44] http://www.zdnet.com/hackers-allege-mt-gox-ceo-still-controls-stolen-bitcoin-7000027137/

[45] Blockchain.info. accessed: 12.5.2014

כפי שניתן לראות בגרף לעיל, חלה התאוששות בערך הביטקוין בחודשים האחרונים לאחר השפל שבעקבות נפילת MtGox. ניתן להסביר התאוששות זו במספר דרכים. ראשית, כתוצאה של אופטימיות מחודשת לגבי עתיד הביטקוין לאור העובדה ששרד את משבר MtGox שרבים צפו שיביא לחיסולו. שנית, כתוצאה של שורה של פרסומים חדשותיים חיוביים: הודעה של הבנק המרכזי הסיני על כך שלא יהיה איסור על שימוש בביטקוין במדינה, שורה של חברות קמעוניות גדולות שהחלו לאפשר רכישה באמצעות ביטקוין ועלייה בהתעניינות בביטקוין ובתדמית שלו כנכס לגיטימי בעקבות המכירה הפומבית שביצע ה-FBI של 300 אלף מטבעות.

פעילות רבה מתקיימת בביטקוין כהשקעה ומאמצים רבים מושקעים בניסיונות לחזות את הערך העתידי שלו. דרך אחת מתבססת על הטענה שבהינתן כמות קבועה של מטבעות שיונפקו, ערכו של המטבע הדיגיטלי קשור לסך הנכסים שניתן לקנות בו ולמהירות המחזור בו. דרך אלטרנטיבית שהוצעה על ידי אנליסטים היא להקביל אותו לזהב שהוא כיום האמצעי המרכזי בעולם לשמירת ערך (store of value)[46]. יחד עם זאת, יש הטוענים שקיימת חוסר ודאות לגבי אמינות ההתחייבות להגביל את מספר המטבעות ל-21 מיליון וגם לגבי הנכסים שיהיה ניתן לרכוש באמצעות הביטקוין.

בנוסף, הצלחת ביטקוין כבר כיום גורמת להקמה של עשרות מטבעות דיגיטליים נוספים שיכולים לנגוס בערך שלו ולפגוע בתפוצת השימוש בו. מצב של ריבוי מטבעות דיגיטליים מתחרים עשוי למנוע מכל אחד מהם תפוצה רחבה מספיק כדי להתבסס כאמצעי חליפין מקובל. מצד זה יביא להיעדר של תועלות רשתיות (network externalities) אצל כל המטבעות המתחרים. תועלות רשתיות אלו נחשבות למאפיין הכרחי של אמצעי חליפין, והן קיימות אצל כל מטבע מדינתי.

בהקשר הזה עולה הטענה שאם צודקים המנבאים שהביטקוין לא יוכל בטווח הארוך לשמש כמטבע, ערכו כהשקעה ירד באופן משמעותי. אולם, כל עוד עתיד ביטקוין לוט בערפל, לצרכינו כאן ניתן להמשיך להתייחס אליו כאמצעי השקעה.

לצד האפשרות להשקיע בביטקוין באופן ישיר (מסחר בביטקוין), מתחילה להתפתח גם האפשרות להשקיע בביטקוין באופן עקיף. זה מתאפשר בדרכים שונות: ראשית, באמצעות מספר מכשירים פיננסיים שקיימים כבר כיום כגון Bitcoin Investment Trust המאפשרת לקנות בה יחידות שמגלמות החזקה עקיפה של ביטקוין מבלי שהמשקיע נדרש להחזיק ביטקוין ברשותו; שנית, באמצעות אפשרויות המסחר באופציות ביטקוין שמציעות פלטפורמות המסחר כדוגמת CoinHedger; שלישית, באמצעות מסחר בחוזים עתידיים הנקובים בביטקוין באמצעות אתרים כגון iCBIT; רביעית, באמצעות מסחר ב-CFD על ביטקוין שמציעים מגוון ברוקרים כגון Plus500. בנוסף, ETF שיאפשר גם כן השקעה עקיפה בביטקוין נמצא בתהליכי אישור רגולטורי בארה"ב[47]. ה- ETF צפוי להיות המכשיר הפיננסי הראשון בביטקוין שייסחר בבורסות רגילות[48].

[46] http://www.coindesk.com/bitcoin-price-reach-98500-say-wall-street-analysts/

[47] http://www.marketwatch.com/story/do-bitcoins-belong-in-your-retirement-portfolio-2013-08-29?pagenumber=2

[48] http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

השקעה במניות באמצעות ביטקוין בשוק ההון מתאפשרת ב-MPEx, בורסה שבה מניות של חברות נסחרות בביטקוין. מדובר בחברות ספציפיות שמונפקות בבורסה הזו. עלות פתיחת חשבון בMPEx היא 30 ביטקוין. כל התשלומים והפדיון גם הם בביטקוין. יש כרגע 4 מניות ועוד מספר ניירות ערך נוספים שנסחרים בפלטפורמה זו, כולם בבעלות מלאה או חלקית של אותו גורם המפעיל את הפלטפורמה. Coinbr הוא ברוקר שמאפשר לסחור ב-MPEx בלי לפתוח חשבון.

פיתוחים נוספים על גבי פלטפורמת ביטקוין

מספר יוזמות חדשות (כגון Colored Coins, Bitshares, Mastercoin) מפתחות רמה חדשה של פונקציונאליות על גבי פלטפורמת הביטקוין. מדובר על פיתוחים שחלקם נמצאים עדיין בשלב רעיוני ולכן לא ניתן לוודא בשלב זה שקיימת היתכנות טכנולוגית או כלכלית למימושם. יחד עם זאת, קיים סיכוי לא מבוטל שפיתוחים אלה מסמנים את כיוון ההתפתחות של המטבעות הדיגיטליים בשנים הקרובות והם יכולים להיות בעלי השלכות רגולטוריות מרחיקות לכת.

יוזמות אלה דומות בכך שהן משתמשות בשיטת שרשרת הבלוקים, לרבות וידוא העברה על ידי כורים באמצעות הוכחת עבודה (למידע נוסף אודות הוכחת עבודה, ראה נספח 1) על מנת לקבוע בעלות על פריטים ברשת. החידוש כאן קשור בכך שבמקום רשת של פריטים הומוגניים, כמו פריטי הביטקוין שכל אחד מהם נועד לייצג מטבע, הרשת יכולה לכלול פריטים שונים שהבעלות עליהם נקבעת באותו אופן.

דוגמא לסוג כזה של פריט היא "נכס חכם", מושג המתייחס לכל נכס שהבעלות עליו נקבעת באמצעות מערכת של שרשרת בלוקים. בנכסים פיזיים כמו רכבים רעיון זה יכול להיות מיושם על ידי מערכת נעילה אוטומטית המתחברת לשרשרת הבלוקים ומזהה את הבעלים שלה. שכלול של רעיון זה הוא "חוזה חכם", שמאפשר להתנות את השליטה בנכס חכם. מכשיר זה מאפשר להפוך את הנכס לערבון כנגד הלוואה, כך שאם ההלוואה לא נפרעת במועד, החוזה החכם משתמש בשרשרת הבלוקים כדי להעביר את השליטה בנכס החכם למלווה.

סוג נוסף של חוזה חכם הוא חשבון השלושה (Escrow Account) המאפשר הפקדה בנאמנות בשותפות עם צד ג' כך שאותו צד ג' מכריע למי עובר הכסף לאחר שתנאי מסוים מתקיים. מערכות שונות אף מאפשרות לייצר צד ג' ממוחשב שיאפשר יישוב סכסוכים ללא צורך באמון כלל. לדוגמא, חברת Ripple Labs הציגה פלטפורמה חדשה לפיתוח חוזים חכמים. הפלטפורמה מאפשרת לייצר את מה שנקרא Smart Oracle, תוכנה שיכולה לבצע חוזה באופן אוטומטי כאשר היא מקבלת את קלטים שהוגדרו מראש. כלי זה עשוי לאפשר ליצור מערכת חוזים נטולת אמון.[49] אמצעי זה הוא היסוד ליצירה של שוק אגרות חוב על גבי אותה רשת, ובאופן דומה, של שוק מניות ושל שווקים נוספים בסוגים מגוונים של חוזים ומכשירים.

אמצעי לצדק חלוקתי

שני מטבעות שצפויים להיכנס לפעילות במהלך שנת 2014, האחד באיסלנד[50] (AuroraCoin) והשני בישראל[51] (IsraCoin), משתמשים בשיטה של הפצה מוקדמת לקבוצה רחבה של אזרחים על מנת לזרז את

[49] http://www.coindesk.com/ripple-labs-unveils-proposal-new-smart-contract-system/

[50] http://www.theverge.com/2014/3/25/5546192/icelanders-can-now-each-claim-400-worth-of-auroracoin-cryptocurrency

[51] http://www.telecomnews.co.il/%D7%94%D7%9E%D7%98%D7%91%D7%A2-%D7%94%D7%95%D7%95%D7%99%D7%A8%D7%98%D7%95%D7%90%D7%9C%D7%99-

אימוץ המטבע הדיגיטלי ותוך הצהרה שכוונתם ליצור צדק חלוקתי באמצעות המטבעות החדשים. החלוקה המוקדמת של מטבעות לקבוצה רחבה של אזרחים מן השורה, ולבעלי עסקים במקרה של המטבע הדיגיטלי הישראלי, מגדילים את הסיכון לאימוץ המטבע. מאפיין זה יוצר ציפייה לאימוץ מהיר ולכן לערך גבוה יותר של המטבע הדיגיטלי. כך עשוי להיווצר מעגל של היזון חוזר חיובי שבו הגידול בערך המטבע הדיגיטלי מגדיל את הסיכוי שהאזרחים להם הוא הונפק יעשו בו שימוש, והציפייה שיותר אזרחים יעשו בו שימוש מגדיל את הערך של המטבע הדיגיטלי בעיני ספקולנטים. מעגל מסוג זה עשוי להיות הגורם לעלייה החדה בערך המטבע האיסלנדי טרם הנפקתו לכדי שווי שוק כולל של 125 מיליון דולר בחודש מרץ 2014. אולם, לפחות במקרה של אוריאקוין, נראה שהתחזיות האופטימיות המוגזמות התבדו. ערך המטבע ירד בצורה חדה מאוד משיא של 70 דולר בתחילת מרץ 2014, ל-50 סנט באמצע מאי 2014, ומאז ממשיך להידרדר באיטיות. ככל הנראה שזוהי תוצאה של תשתית מחשובים לא מתאימה, היעדר תמריץ לכרייה, וספקולציה נרחבת שגרמה לירידת ערך ואז למכירה של מרבית המטבעות שהועברו לאזרחים.

השימוש בישראל

לא קיים מידע מסודר על השימוש בישראל במטבעות דיגיטליים אך מחיפוש באינטרנט ניתן להתרשם שקיימת קהילה תוססת של משתמשים בישראל. לפי אתר קהילת הביטקוין של ישראל, 113 עסקים מקבלים ביטקוין בתמורה לסחורה ולשירותים בישראל, גידול של 35% בתוך ארבע חודשים[52]. היקף השימוש במטבעות דיגיטליים אחרים אינו ברור.

דיווחים של פעילים בקהילה מצביעים על קשיים שמעלה המערכת הבנקאית מול המשתמשים במטבע הביטקוין. לפי אותם דיווחים, קבוצת הבנק הבינלאומי החליטה לא לאפשר ללקוחות עסקיים או פרטיים להעביר כספים לבורסת MtGox למטרת קניית ביטקוין[53]. פעילים בקהילת הביטקוין הישראלית נתקלו בסירוב משורה של בנקים בישראל (הבינלאומי, מזרחי טפחות, בנק הפועלים, בנק דיסקונט, בנק לאומי) לעשות פעילות בביטקוין בחשבון שלהם, לרבות העברת כספים לפלטפורמות למסחר בביטקוין כמו MtGox.

עו"ד אורי גולדמן ממשרד עורכי הדין גולדמן ושות' מייצג כמה וכמה אתרי המרת מטבע ישראליים הנותנים שירותי המרת מטבע בין מטבעות מדינתיים למטבעות דיגיטליים. לדבריו נפח המסחר של לקוחותיו הוא כ-3 מיליון שקל בשבוע. בנוסף, קיימים בישראל שירותים שמאפשרים השקעה בביטקוין ובמטבעות אחרים. למשל, Bit2C היא פלטפורמת מסחר למטבעות דיגיטליים המופעלת בישראל; Bitsofgold ועוד מספר חברות בישראל מפעילות שירותי חליפין שמאפשרים לישראלים לרכוש ביטקוין. בנוסף, ישראל מהווה מוקד חדשנות בתחום הביטקוין כאשר יוזמות כגון Mastercoin ו-Colored Coins שהוזכרו לעיל מבוססות בישראל.

%D7%94%D7%99%D7%A9%D7%A8%D7%90%D7%9C%D7%99-Isracoin-%D7%99%D7%A6%D7%90-%D7%94%D7%99%D7%95%D7%9D-%D7%9C%D7%93%D7%A8%D7%9A.html

[52] http://wiki.bitcoin.org.il/index.php/%D7%A8%D7%A9%D7%99%D7%9E%D7%AA_%D7%A2%D7%A1%D7%A7%D7%99%D7%9D_%D7%94%D7%9E%D7%A7%D7%91%D7%9C%D7%99%D7%9D_%D7%91%D7%99%D7%98%D7%A7%D7%95%D7%99%D7%9F_%D7%91%D7%90%D7%A8%D7%A5 accessed: 11.5.2014, 11.2.2014.

[53] http://rotter.net/forum/scoops1/43097.shtml

יחס הרגולטורים בעולם ובישראל

שיקולים רגולטוריים מרכזיים

רגולטורים, בתי מחוקקים וגורמי אכיפת חוק עומדים בפני אתגר מורכב בבואם לעצב את הסביבה הרגולטורית של המטבעות הדיגיטליים. מחד, ישנן סכנות פוטנציאליות משמעותיות (שיפורטו מיד) ומדינה שלא תשכיל להתייחס לכך עלולה לצאת נפגעת מכך. מאידך, קיים גם פוטנציאל גדול לחדשנות טכנולוגית ופיננסית ומדינה שתייצר רגולציה כובלת מדי עלולה לדחוק החוצה טכנולוגיה חדשה שעשויה להתברר כמנוע צמיחה עתידי.

את האתגרים העומדים בפני רגולטורים לאור הכניסה לשימוש של מטבעות דיגיטליים נחלק בעבודה זו לשם נוחות לאתגרים מיידים ופוטנציאליים. אתגרים מיידים הם אותם אתגרים הרלוונטיים באופן מידי בהיקף השימוש הנוכחי של המטבעות או בהיקף השימוש שאליו הם צפויים להגיע בזמן הקרוב. אתגרים פוטנציאליים הם אותם אתגרים שיעמדו על הפרק במידה והיקף השימוש במטבעות יתרחב באופן משמעותי.

הצורך לאזן בין שני השיקולים של צמצום סיכונים מחד וניצול היתרונות מאידך, עלתה במספר ניירות עמדה בנושא, כמו גם בעדויותיהם של גורמי ממשל שונים בפני הקונגרס האמריקני במסגרת השימוע שנערך בנושא מטבעות דיגיטליים. נפתח את סקירת הסיכונים בסיכון רלוונטי במיוחד לתפקידן של רשויות לניירות ערך – אינטראקציה אפשרית של ביטקוין, ושל מטבעות דיגיטליים בכלל, עם שווקי ההון בארץ ובעולם.

אינטראקציה עם שווקי ההון בעולם

על מנת למפות את האפיקים השונים דרכם יכולים ביטקוין ומטבעות דיגיטליים אחרים להשפיע על שווקי הון בעולם, נתבונן בשימושים השונים של מטבעות דיגיטליים בפרק הקודם. אפיק השקעה כלשהו יכול להשפיע על שווקי הון דרך השפעתו על מדדים או דרך השפעתו על הרכב הנכסים של גופים שונים. כיום למטבעות הדיגיטליים אין השפעה ישירה על מדדים משום שעדיין לא קיים מוצר העוקב אחרי הערך שלהם שנסחר בבורסה כלשהי לניירות ערך. כמו כן, השפעתם על הרכב הנכסים גם היא מצומצמת משום שאפשרויות ההשקעה במטבעות דיגיטליים היא מצומצמת.

מטבע יכול להשפיע על שווקי הון בעיקר דרך ניירות ערך המתומחרים בו כגון ניירות ערך ומניות. במקרה של מטבעות דיגיטליים אין ניירות ערך כאלה. אפיק השפעה נוסף הוא דרך המאזנים של גופים פיננסיים, בעיקר של בנקים. חיפוש באינטרנט לא איתר אפשרויות לקבל הלוואות בנקאיות בביטקוין או להפקיד ביטקוין בבנקים מסורתיים. קיימים דיווחים לא מאושרים על כך שבנקים גדולים ברחבי העולם לא מאפשרים ללקוחות לרכוש או לעשות כל פעילות אחרת הקשורה לביטקוין באמצעות חשבונות הבנק שלהם[54]. גורמים בעיתונות הכלכלית, כדוגמת אתר האינטרנט של העיתון פורבס, מסבירים התנהלות זו, לפחות של הבנקים בארה"ב, כתוצאה של שתי הנחיות ממשלתיות שפורסמו בשנת 2013 – האחת המגדירה את כל העסקים העוסקים הסוחרים בביטקוין כ"עסקי שירותי כסף" (money services businesses), והשנייה הגדירה את העסקים העוסקים בביטקוין כעסקים בעלי סיכון גבוה. ההגדרה של "עסקי שירותי

[54] http://markmaunder.com/2013/12/05/banks-declaring-war-on-bitcoin/

כסף״ חלה על כל הגורמים העוסקים בהעברה או בחלפנות של כסף ומחילה על בתי עסק אלו דרישות של רישום, דיווח ואמצעים שונים למניעת הלבנת כספים, וגם מטילה חובות רגולטוריות מוגברות על הבנקים הנותנים להם שירות. הפחד מרגולציה עודפת ומהסיכון הגבוה של העסקים עשוי להיות הגורם להתנגדות הבנקים לביטקוין. כמו כן, יתכן שמבלי אישור מפורש מהבנק המרכזי לטפל בחשבונות ביטקוין, הבנקים לא רואים את עצמם רשאים לעשות זאת. לצד טיעונים אלה נשמעים טיעונים לגבי הפחד של הבנקים מהביטקוין שנוצר לכאורה כדי לייתר אותם.[55] [56] לאור מידע זה, ניתן להסיק שלא סביר שתוכל להיות השפעה של מטבעות דיגיטליים על מאזנים של בנקים ועל יציבותם.

השפעות עקיפות יותר של מטבעות דיגיטליים על שווקי ההון יכולים לנבוע מהשפעת הטכנולוגיה החדשה שהמטבעות הדיגיטליים מציעים על תפקידם של המטווחים הפיננסיים המסורתיים כדוגמת חברות אשראי, בנקים, ברוקרים, מסלקות ובורסות. השפעות אלה יוכלו להתממש במידה ויתגבר השימוש במטבעות הדיגיטליים באופן משמעותי ולכן נדון בנושא הזה בחלק של ״אתגרים פוטנציאליים״.

הזדמנויות

להלן כמה מההזדמנויות שעלו מהספרות האקדמית והעיתונאית לגבי ההזדמנויות והיתרונות שעשויים לצמוח כתוצאה ממטבעות דיגיטליים:

- מטבעות דיגיטליים עשויים לטפח חדשנות פיננסית
- הגברת המהירות והורדת העלות של מערכות תשלום[57]
- הורדת עלויות עסקה בכלכלה
- עידוד נגישות לשירותים פיננסיים בעולם המתפתח
- הזדמנויות למשקיעים לגוון את תיקי ההשקעות שלהם
- אמצעי לשמירת ערך ואף צבירת ערך הודות לאופיים הדיפלציוני של מטבעות דיגיטליים כמו ביטקוין
- עשויים לצמצם את הפגיעה במדינה מסוימת כתוצאה ממדיניות מוניטארית פוגענית של מדינות אחרות

אתגרים מיידיים

כאמור, אתגרים מיידים הם אותם אתגרים הרלוונטיים באופן מידי בהיקף השימוש הנוכחי של המטבעות או בהיקף השימוש שאליו הם צפויים להגיע בזמן הקרוב.

---

[55] http://www.forbes.com/sites/kashmirhill/2013/11/15/bitcoin-companies-and-entrepreneurs-cant-get-bank-accounts/

[56] http://www.equities.com/editors-desk/stocks/financials/why-aren-t-investment-banks-getting-into-bitcoin

[57] http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

- סוגיית **ההגדרה של האמצעים הטכנולוגיים החדשים** עשויה להיות מרכזית במאמץ לעצב סביבה רגולטורית מתאימה[58]. האם ביטקוין, למשל, הוא מטבע, נייר ערך או שניהם? האם כורים הם ספקים של שירותים פיננסיים?
- כמו כן, עומדת על הפרק גם שאלת **המיסוי**[59]. האם יש חובה לשלם מע"מ על עסקאות בביטקוין? האם כורה מחויב במס הכנסה על פעילותו? האם רווחים ממסחר בביטקוין הם רווחי הון?
- **סכנה לאובדן כספי משקיעים**, היא אחד האתגרים הראשונים שזכו להתייחסות הרגולטורים[60]. סכנה כזו יכולה להתממש במגוון דרכים (שחלקן אכן התממשו בחודשים האחרונים): ראשית, זירות המסחר שבהן אנשים סוחרים במטבעות דיגיטליים ושירותי הארנק שבהם הם מאכסנים את החשבון הפרטי שלהם, סובלים מחוסר יציבות ומבעיות אבטחת מידע. תקלות טכניות, התערבויות רגולטוריות והתקפות ממוחשבות גרמו בשנה האחרונה לכמה מהזירות הגדולות ביותר להפסיק לפעול או לא לאפשר משיכת כספים מהן לטווחי זמן שונים. כמו כן, מטבעות דיגיטליים בסכומים גדולים נגנבו מהשירותים הללו. גניבות כאלה מתבצעות גם מאנשים פרטיים. שנית, משום שערכם של המטבעות הללו לא מגובה על ידי גורם ריבוני כלשהו, הם עלולים לאבד את ערכם כתוצאה מהתנפצות בועה או מסיבות אחרות. כמו כן, לאחרונה עולה הטענה כי רשת הביטקוין אינה חסינה בפני מניפולציות, בייחוד על ידי גורמים המחזיקים בחלק משמעותי מרשת הכורים. בריכת הכורים GHash הגיעה ל-55% מכוח המחשוב של רשת הביטקוין בחודש יוני, מצב שאפשר לה לבצע התקפות העברה כפולה עם סיכוי גבוה מאוד להצלחה. כדי למנוע פאניקה מפני השתלטות של הבריכה של רשת הביטקוין, הרשת הודיעה שהיא מגבילה באופן וולונטארי את כוח המחשוב שלה ל-39.99%. אולם פתרון זה נחשב ללא יציב משום שהוא מבוסס על רצונה הטוב של הבריכה ולא על מערך תמריצים, כך שבריכות אחרות עלולות שלא לפעול באופן כה אדיב. בינתיים הוצעו מספר פתרונות טכנולוגיים כדי להפוך את רשת הכורים ליותר מבוזרת, אולם עדיין לא ברור איזה מהם אם בכלל יתקבל על ידי הקהילה. [61]
- המורכבות הטכנולוגית וההילה החדשנית שאופפת מטבעות כמו הביטקוין הופכת אותם **לאמצעי יעיל עבור רמאים על מנת לבצע הונאות שונות**[62].
- בנוסף לסכנה לכספי משקיעים, אתגר נוסף בהקשר זה הוא לוודא **שיש ביכולתם של גורמי אכיפת החוק לחקור ולהרשיע רמאים אלה** על בסיס החוקים הקיימים שאינם בהכרח מותאמים למטבעות דיגיטליים[63].
- שימוש במטבעות דיגיטליים ככלי חדש **להלבנת הון** היא אחד החששות המרכזיים של רגולטורים בעולם[64]. החשש עולה עקב האפשרות לבצע העברות כספים במטבעות דיגיטליים בין חשבונות שזהות בעליהם אינה יידועה לאף גורם שלישי.
- **עקיפת הגבלות על תנועות** הון גם היא מתאפשרת כיום לאור היעדר הרגולציה והיעדרם של גורמי צד ג' המעורבים בהעברת כספים[65].

---

[58] p200 http://hstlj.org/wp-content/uploads/2011/12/8-Grinberg-159-208.pdf

[59] http://www.gao.gov/assets/660/654620.pdf

[60] http://www.ynet.co.il/articles/0,7340,L-4490067,00.html

[61] /http://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue

[62] https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

[63] http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

[64] http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

- **סכנת מסחר לא חוקי** מהווה אתגר נוסף. אפשרות המסחר ללא חשיפת זהות הסוחר מאפשר מסחר במוצרים לא חוקיים או על ידי גורמי פשיעה[66].
- כתוצאה מהרישום הפומבי של כלל הטרנסאקציות, קיימת סכנה **לפרטיות המשתמשים** במידה והכתובות הפומביות שבהן עשו שימוש נקשרות באופן פומבי לזהותם[67].

אתגרים פוטנציאליים

אתגרים פוטנציאליים הם אותם אתגרים שבהווה אינם עומדים על הפרק אך שעשויים להפוך לרלוונטיים כתלות בהיקף ואופן השימוש במטבעות דיגיטליים.

- **איומים לכלכלה בכללותה** כוללים בין השאר: ספירלה דיפלציונית שיכולה במצב קיצוני להיגרם על ידי האופי הדיפלציוני של הביטקוין ושל מטבעות דיגיטליים אחרים בעלי היצע מוגבל וחוסר היכולת להתערב בהיצע שלהם[68]; אובדן הבלעדיות של כסף מדינתי בתור אמצעי התשלום במשק יכולה ליצור פגיעה במקרה ותתערער היציבות התפעולית של רשת הביטקוין[69] או במקרה שרשת הביטקוין תיחטף על ידי גורמים עוינים (אפשרות שהועלתה לאחרונה על ידי מדען מחשב מאוניברסיטת קורנל[70]).
- **שיבוש במדיניות מאקרו כלכלית** הוא תוצאה אפשרית של התרחבות השימוש במטבעות דיגיטליים מבוזרים, עד כדי הפיכתם לאמצעי חליפין שמתבצע בו חלק משמעותי מהטרנסאקציות במשק. שיבושים אפשריים כוללים ראשית, פגיעה ביכולת הבנק המרכזי לשלוט בצורה אפקטיבית בשער הריבית. מצב זה יכול לנבוע מהיווצרות קווי אשראי אלטרנטיביים[71], מקושי למדוד את מהירות המחזור של הכסף[72] או מקושי לשלוט כמות אמצעי התשלום במשק[73]; שנית, יצירת קשיים בהערכת כמות הכסף ובחיזוי הקשר בינה לבין קצב האינפלציה[74]; שלישית, סכנה לאמינות ולמוניטין של הבנק המרכזי במקרה של כשל כלשהו בביטקוין בגלל תפיסת הציבור שפיקוח על מטבעות דיגיטליים הוא באחריות הבנק המרכזי[75].
- **שינוי במבנה שווקי ההון והשלכות לגבי תפקידם של המתווכים הפיננסיים הקלאסיים.** אופן השימוש במטבעות דיגיטליים, עשוי למצמצם אם לא לבטל את הצורך בחלק מהמתווכים הפיננסיים הקלאסיים. סכנה זו הועלתה על ידי גורמים שונים בייחוד ביחס למתווכים כגון חברות כרטיסי האשראי ושירותי העברת כספים. אולם יש הטוענים כי השינוי עשוי להיות מורגש

---

[65] The Library of Congress. Regulation of Bitcoin in Selected Jurisdictions, Jan 2014.

[66] http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

[67] http://anonymity-in-bitcoin.blogspot.co.il/2011/07/bitcoin-is-not-anonymous.html

[68] ספירלה דיפלציונית: מצב שבו העלייה בכוח הקנייה של הכסף יוצרת תמריץ לאגירתו שמגדילה פעם נוספת את כוח הקנייה שלו[68] (ניסיון להפריך כיוון חשיבה זה ניתן למצוא ב[68])

[69] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[70] http://hackingdistributed.com/2013/11/04/bitcoin-is-broken/

[71] http://www.fas.org/sgp/crs/misc/R43339.pdf

[72] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[73] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

[74] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf, p35

[75] http://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

גם בחלק מהפעילות של בנקים ויתכן אף שינוי בתפקיד המתווכים בשוק ההון כגון הבורסות, המסלקות וזירות המסחר[76].

הרגולציה בעולם ובישראל

רגולציה בארה"ב

ה-IRS (Internal Revenue Service), פרסם במרץ 2014 הנחיות הקובעות שהיחס למטבעות דיגיטליים יהיה בדומה ליחס לרכוש (property), מה שגורר חובות דיווח נרחבות על טרנסאקציות בביטקוין וחובות מס על כרייה של מטבעות דיגיטליים, קבלת שכר במטבעות דיגיטליים, רכישה או מכירה של נכסים בתמורה למטבעות דיגיטליים. הדיווח יתבצע לפי השווי ההוגן של המטבע הדיגיטלי שיחושב לפי שער ההמרה של המטבע הדיגיטלי מול הדולר ביום קבלתו בפלטפורמת מסחר המפרסמת שער הנקבע לפי ביקוש והיצע[77]. דבר זה הביא כמה פרשנים להכריז על סופו של הביטקוין בארה"ב כתוצאה מחובות הדיווח הנוקשים שההנחיה מחילה[78].

ה-SEC (Securities and Exchange Commission), פרסם ביולי 2013 הודעת אזהרה למשקיעים בנוגע לסיכונים של הונאות המערבות מטבעות וירטואליים. במסגרת ההודעה צוין כי כל השקעה בניירות ערך בתחומי ארה"ב נופל תחת סמכות הפיקוח של ה-SEC, גם אם ההשקעה מתבצעת במטבעות וירטואליים. בנוסף, צוין גם כי גורמים המוכרים השקעות מחויבים בדרך כלל ברישיונות ברמה המדינתית או הפדראלית.[79] במכתב לקונגרס ציינה יו"ר ה-SEC כי כל ישות המחזיקה בבעלות מטבעות וירטואליים המנפיקה מניות או ניירות ערך מסוג כלשהו או המספקת החזר על השקעות בהתבסס על נכסים כגון מטבעות וירטואליים נמצאת תחת הפיקוח של ה-SEC. כמו, התייחס המכתב למוצרים פיננסיים שיסחרו בבורסה ארצית לניירות ערך (national securities exchange) שיתבססו באופן כלשהו על מטבעות וירטואליים. לפי המכתב, על מנת שמסחר כזה יתאפשר, אותה בורסה צריכה לפנות ל-SEC ולבקש שינוי כלל (rule change) שיאפשר את הרישום ואת המסחר במוצר באותה בורסה.[80]

FinCEN (Financial Crimes Enforcement Network), פרסם במרץ 2013 הנחיות רשמיות שמחייבות את כל העסקים הפועלים במסחר במטבעות וירטואליים להירשם כ-MSB (Money Services Business), מה שמחייב אותם לרישום, דיווח, ותיעוד פעולות כמו גם לנקוט אמצעים נגד הלבנת כספים ולהפעיל מדיניות להכרת לקוחותיהם (know-your-customer)[81]. רגולטורים של מדיניות בתוך ארה"ב, כגון

---

[76] http://static.squarespace.com/static/51df1ba4e4b08840dcfce197/t/5212ca63e4b0348bfd2276c6/1376963171729/BitShares%20White%20Paper%20(2).pdf

[77] http://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance

[78] http://finance.yahoo.com/blogs/talking-numbers/this-could-be-the-end-of-the-bitcoin-era-220746326.html

[79] https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

[80] http://online.wsj.com/public/resources/documents/VCurrenty111813.pdf

[81] http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html

קליפורניה וניו יורק, פרסמו כללים באותה רוח.[82] בסוף ינואר 2014, פרסם FinCEN הבהרות לגבי הנחיות אלו, לפיהן הגורמים הבאים לא נדרשים להירשם כ-MSB: א. כורים או אנשים אחרים המייצרים מטבעות וירטואליים לשימושם האישי; ב. אנשים המייצרים או המפיצים תוכנות שנועדו לסייע למכור או לקנות מטבעות וירטואליים; ג. אנשים שקונים או מוכרים מטבעות וירטואליים למטרות השקעותיהם האישיות בלבד.[83]

ה-FED (Board of Governors of the Federal Reserve System), מסר שבהינתן אופן ההפעלה הנוכחי של מטבעות וירטואליים, הם ל**א נמצאים תחת אחריותו הרגולטורית** ואין בסמכותו לפקח עליהם.[84] לפי מכתב מיו"ר ה-FED לקונגרס, מצב זה ימשך כל עוד הסליקה וההנפקה של המטבעות הווירטואליים מתבצעת דרך רשת מבוזרת וללא אינטראקציה עם גופים המפוקחים על ידו (בנקים בארה"ב)[85].

ה-GAO (Government Accountability Office), פרסם במאי 2013 מסמך המבקש מה-IRS (Internal Revenue Service) לפרסם הנחיות בנוגע למיסוי מטבעות וירטואליים על מנת להפחית את הסיכונים להם חשופים גורמים בתחום כתוצאה מחוסר ודאות לגבי חובות המס שלהם[86]. המסמך לא הגדיר באופן מפורש כיצד ובאילו קטגוריות המיסוי צריך להתבצע.

ה-**FBI (Federal Bureau of Investigation)**, בתחילת 2012, הקימה ועומדת בראשה של קבוצת עבודה בין משרדית תחת הכותרת "Virtual Currency Emerging Threats Working Group" שנועדה להתמודד עם האיומים החדשים העולים בתוצאה מהשימוש הגובר במטבעות וירטואליים.

ה- FEC (Federal Election Committee) **אישרה לקבל תרומות** פוליטיות בביטקוין תחת הקטגוריה הכוללת סחורות, מניות וציוד **אך לא תחת הקטגוריה של כסף**, מה שמחייב שתרומות בביטקוין יומרו לדולרים לפני הפקדה לחשבון המקבל[87].

לפי הסיקור החדשותי, בדיוני ועדות של **הסנאט האמריקאי** בנושא מטבעות וירטואליים הגישה הפופולארית הייתה שיש לפקח עליהם אך בצורה שלא תפגע בתמריץ לחדשנות הנובע מהמטבעות הווירטואליים ולא תדחוף את היזמים לפעול בשווקים בהם הרגולציה פחות נוקשה. בנוסף, עולה מהסיקור כי הרגולטור האחראי על מניעת הלבנות הון ומימון טרור בארה"ב (FinCEN) מאמין כי התשתית המשפטית הקיימת מהווה פלטפורמה מספקת להתמודדות עם תופעת המטבעות וירטואליים בהקשרים הללו. כמו כן, עולה כי ביטקוין ומטבעות דיגיטליים מבוזרים נוספים המשתמשים בתיעוד עסקאות פומבי,

---

82 http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

83 http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf

84 http://online.wsj.com/public/resources/documents/VCurrenty111813.pdf

85 http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

86 http://www.gao.gov/assets/660/654620.pdf

87 http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

שעומדים במרכז עבודה זו, לא מהווים אמצעי אטרקטיבי עבור עבריינים, בניגוד למטבעות דיגיטליים ריכוזיים המופעלים על ידי גורמים הפועלים במודע לעקוף רגולציה ולמנוע מעקב[88].

מדינת ניו-יורק, באמצעות המחלקה לשירותים פיננסיים, פרסמה מסמך נהלים בנוגע למטבעות דיגיטליים להתייחסות הציבור. המסמך מטיל דרישות רגולטוריות מקיפות על חברות העוסקים במטבעות דיגיטליים. הרגולציה תחול על חברות אשר מאכסנות, מעבירות, ממירות, או מקבלות מטבעות דיגיטליים עבור לקוחות, מוכרות או קונות מטבעות דיגיטליים עבור לקוחות, מנהלות או מנפיקות מטבעות דיגיטליים או ממירות מטבעות דיגיטליים למטבעות מדינתיים וחזרה. היא לא תחול על סוחרים המקבלים מטבעות דיגיטליים בתמורה למוצרים או שירותים. הדרישות יכללו רישוי על ידי המדינה, תיעוד כל הטרנסאקציות, וידוא זהות הלקוחות ודרישות נוספות בתחומים כגון מניעת הלבנת כספים וביקורת כספים שנתית. [89]

קיימת כרגע חוסר ודאות לגבי עמדת **FDIC**, הגוף הפדרלי שתפקידו לבטח את פיקדונות לקוחות הבנקים, לגבי המעמד של ביטקוין. לפי טענה בלתי מאושרת, בהודעה לבנקים, שככל הנראה לא פורסמה באופן פומבי, ניתנו עסקי העוסקים בביטקוין כדוגמא לעסקים מסוכנים. יתכן שזו הסיבה שבנקים בארה״ב לא מאפשרים לעסקים רבים הפועלים בתחום הביטקוין לנהל אצלם חשבון עסקי.

למרות שהביטקוין לא מוגדר בארה״ב ככסף, רשויות אכיפת החוק ניהלו לאחרונה מספר תיקים בהם פסק הדין התייחס לביטקוין ככסף. למשל, במשפט נגד אדם שהפעיל שוק שחור באינטרנט שעשה שימוש בביטקוין כאמצעי תשלום[90]. בנוסף, שופט מחוזי בארה״ב הגדיר אותו ככסף בפרשת הונאת הפונזי בביטקוין[91]. באותו מקרה, השופט אף פירש את ההצעה של מנהל הונאת הפונזי ללקוחותיו כהשקעה בנייר ערך. זאת בהתבסס על הגדרת ניירות ערך (securities) בארה״ב, בין השאר כ״חוזי השקעה״ (investment contracts).

בהקשר זה חשוב לציין שהחוק בארה״ב אוסר על יצירת תחרות לדולר[92], ולפיכך היחס למטבעות דיגיטליים עשוי להשתנות במהירות במידה והתחזיות של תומכיהם בדבר הפיכתם למטבעות בשימוש נרחב יתקרבו לידי מימוש.

באחת העבודות האקדמיות הראשונות בנושא, ראובן גרינברג מבית הספר למשפטים של ייל, טוען כי מבחינה משפטית, לפחות ביחס לחוקי ארה״ב, ביטקוין לא נופל באופן חלק לתוך אף אחת מההגדרות של מוצרי ההשקעה השונים[93]. עמדה זו מוצאת לה מספר תומכים, כמו עו״ד גיון ווילאם נלסון, הכותב בנושאי טכנולוגיה ומשפט[94].

---

[88] http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

[89] http://www.coindesk.com/new-york-reveals-bitlicense-framework-bitcoin-businesses/

[90] http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments

[91] http://www.forbes.com/sites/kashmirhill/2013/08/07/federal-judge-rules-bitcoin-is-real-money/

[92] http://hstlj.org/wp-content/uploads/2011/12/8-Grinberg-159-208.pdf, p182

[93] http://hstlj.org/wp-content/uploads/2011/12/8-Grinberg-159-208.pdf p200

[94] http://www.lextechnologiae.com/2011/06/26/why-bitcoin-isnt-a-security-under-federal-securities-law/

רגולציה באירופה

רשות הבנקאות האירופית (EBA) פרסמה הודעת אזהרה חריפה בנושא השקעה במטבעות וירטואליים בטענה שמשקיעים דרך פלטפורמות שיוצאות משימוש עלולים להפסיד את כספם ללא אפשרות לקבלו חזרה[95]. צרפת מסרה הודעת אזהרה דומה לבנקים[96].

גרמניה – ביטקוין מוגדר ככסף פרטי (Private Money) וסוחרים בו מחויבים בתשלום מס על רווחי הון[97].

בריטניה – מטבעות דיגיטליים מסווגים כנכסים (assets) או ככסף פרטי (private money). ה-HMRC (Her Majesty's Revenue and Customs) פרסמה הודעה לפיה פעילות כרייה ועמלות שיתקבלו על ידי כורים במסגרת אישור טרנסאקציות לא יחויבו במע"מ, רכישה ומכירה של מטבעות וירטואליים לא תחויב במע"מ. לעומת זאת, רווחים כתוצאה מקנייה ומכירה של מטבעות וירטואליים יחויבו במס חברות במקרה של חברות ובמס הכנסה במקרה של יחידים. מס רווחי הון גם הוא חל על רווחים והפסדים כתוצאה מקנייה ומכירה של מטבעות וירטואליים[98].

שוויץ – רגולציה למניעת הלבנת כספים ומימון טרור חלה על עסקים העוסקים בביטקוין ובפרט על שירותי מסחר בביטקוין. בנוסף, עסקים המקבלים ביטקוין מלקוחות ושומרים אותם בחשבונם מחויבים בקבלת רישיון בנקאות.[99] במקביל, דוח של המועצה הפדרלית (ממשלת שוויץ) קובע שמטבע וירטואלי הוא בהגדרה רכוש (property) וכן, אמצעי תשלום (means of payment), אולם נראה כי לשני מושגים אלו אין מעמד משפטי בחוק השוויצרי. באותו דוח נקבע במפורש שההנחיה לגבי שמירת כספי לקוחות בחשבון העצמי חלה גם על ברוקרים ודילרים העוסקים במסחר בביטקוין ועשויה לחייב אותם לקבל רישיון בנקאי. כמו כן, הדוח שולל את האפשרות שביטקוין יחשב כנייר ערך או כחוזה פיננסי, אך לא שולל את האפשרות שמוצרים פיננסיים המשתמשים בביטקוין כנכס בסיס ייחשבו בעתיד כנגזרים.

נורבגיה – מנהל רשות המיסים הנורווגית מסר לבלומברג כי ביטקוין אינו מטבע אלא נכס. כמו כן, יוטל מס רווחי הון על רווחים הנובעים ממסחר בביטקוין[100].

פינלנד – הבנק המרכזי קבע שביטקוין אינו עונה להגדרה של כסף או של אמצעי תשלום אלקטרוני והגדיר אותו בתור סחורה (commodity)[101]. בנוסף, רשות המיסים של פינלנד פרסמה באוגוסט 2013 מדריך מפורט למיסוי של מטבעות דיגיטליים, לרבות ביטקוין. לפי המדריך, מוטל בפינלנד מס על רווחי הון על מסחר במטבעות דיגיטליים[102] ומס הכנסה על כרייה של ביטקוין[103].

---

[95] http://money.cnn.com/2013/12/13/technology/bitcoin-europe-regulation/

[96] http://articles.economictimes.indiatimes.com/2013-12-08/news/44942904_1_digital-currency-bitcoin-currency-concept

[97] http://www.cityam.com/blog/1390228199/bitcoin-faces-latest-regulation-barrage-time-its-finland

[98] http://www.coindesk.com/top-uk-tax-agency-eliminate-20-levy-bitcoin-trading/

[99] http://www.finma.ch/e/finma/publikationen/faktenblaetter/documents/fb-bitcoins-e.pdf

[100] http://www.finextra.com/news/fullstory.aspx?newsitemid=25547

[101] http://www.cityam.com/blog/1390228199/bitcoin-faces-latest-regulation-barrage-time-its-finland

[102] The Library of Congress. Regulation of Bitcoin in Selected Jurisdictions, Jan 2014.

[103] http://translate.google.com/translate?depth=1&hl=en&ie=UTF8&nv=1&prev=_t&rurl=translate.google.com&sl=auto&tl=en&u=http://vero.fi/fi-FI/Syventavat_veroohjeet/Verohallinnon_ohjeet/Virtuaalivaluuttojen_tuloverotus(28450)

איסלנד – איסור מסחר בביטקוין כחלק מהגבלות על מסחר במט״ח[104].

בפולין, משרד האוצר אישר שחוזים עתידיים ואופציות הנקובים בביטקוין נחשבים למכשירים פיננסיים לפי החוק.[105]

פלטפורמת מסחר בביטקוין Bitcoin-Central תהיה הראשונה שתפעל במסגרת החוק האירופי הודות לרישיון ספק אמצעי תשלום (PSP) של חברת האם שלה Aqoba[106]. רישיון זה מקנה קידומת בנק בינלאומית, ויוצר סטטוס מקביל לשירות התשלומים פייפאל. הגדרה זו מחילה על החברה האם שורה של התחייבויות בתחומים כמו שקיפות, רישום, דיווח ללקוח, הסדרי אחריות, החזרי תשלום, זמן ביצוע מכסימלי וכו׳. אולם, לא ברור כמה מחובות אלה מואצלות מטה לפלטפורמת הביטקוין. בכל מקרה, יתכן שזוהי דוגמא שחברות נוספות בתחום הביטקוין עשויות ללמוד ממנה בניסיונן להגדיל את הודאות הרגולטורית סביב פעילותן.

אליפטיק (Elliptic), שירות כספת למטבעות וירטואליים הודיע בינואר 2014 שהוא מבטח את הכספת שלו אצל אחד הסינדיקטים שפעלים במסגרת שוק הביטוח הוותיק, לוידס אוף לונדון (Lloyd's of London).

רגולציה במדינות נוספות

סין - הבנק המרכזי הסיני ומספר משרדי ממשלה נוספים הוציאו הודעה משותפת לגבי הסיכונים של ביטקוין. ההודעה מגדירה את הביטקוין כ״סחורה וירטואלית״ ואוסרת על שימוש בו כמטבע. לפי ההודעה, למוסדות פיננסיים בסין אסור לתת תמחור בביטקוין, לקנות או למכור ביטקוין, לספק באופן ישיר או עקיף שירותי ביטקוין ללקוחות, לרבות רישום, מסחר, סליקה. בנוסף המכתב קורא להגביר את האכיפה על אתרי אינטרנט העוסקים בביטקוין ומזהיר כנגד סיכונים של הלבנת כספים.[107]

ברזיל - החלה להסדיר בחוק את נושא המטבעות הדיגיטליים. אולם החקיקה מתייחסת לנושא בעיקר דרך הפרספקטיבה של שירותי תשלום ומותירה לבנק המרכזי לקבוע את הפרמטרים לפיהם שירותים כאלה מצופים לנהוג. מהחומר הקיים בנושא באנגלית לא ניכר שהחוק מכריע בסוגיות אחרות כגון מיסוי או אופן הטיפול הנדרש מבנקים במטבעות דיגיטליים.[108]

רוסיה – משרד התובע הראשי הגדיר את הביטקוין, יחד עם מטבעות קריפטוגרפיים נוספים, כתחליף כסף ואסר למעשה על אזרחים ועל עסקים לעשות בו שימוש[109]. אולם, לאחרונה הבנק המרכזי של רוסיה הצהיר כי אין לשלול על הסף שימוש במטבעות דיגיטליים ושהבנק המרכזי לומד כרגע את הנושא ועוקב אחר התפתחויות בתחום לפני קבלת החלטה בנושא.[110]

---

[104] The Library of Congress. Regulation of Bitcoin in Selected Jurisdictions, Jan 2014.

[105] http://www.coindesk.com/polish-finance-ministry-says-bitcoin-can-used-financial-instrument/

[106] http://www.finextra.com/news/fullstory.aspx?newsitemid=24361

[107] http://www.hsgac.senate.gov/media/majority-media/new-report-outlines-treatment-and-regulation-of-bitcoin-around-the-world

[108] http://www.hsgac.senate.gov/media/majority-media/new-report-outlines-treatment-and-regulation-of-bitcoin-around-the-world

[109] http://www.reuters.com/article/2014/02/09/us-russia-bitcoin-idUSBREA1806620140209

[110] http://www.coindesk.com/bank-of-russia-bitcoin-should-not-be-rejected/

ביפן הוקם איגוד לעסקים בתחום המטבעות הדיגיטליים (JADA – The Japanese Authority of Digital Assets). האיגוד הוקם בתמיכת הממשל אך יפעל כגוף עצמאי שתפקידו לאגד את העסקים ולהסדיר את פעילותם על בסיס וולונטארי. צעד זה יכול להיתפס בתור האמצעי של ממשלת יפן להבטיח פיקוח על פעילות הגופים בתחום מבלי לכפות רגולציה מלמעלה.[111]

קנדה – חוקי המס חלים על ביטקוין. זה כולל הן מס על רווחי הון ממסחר בביטקוין והן מס על סחר חליפין (barter transactions) ברכישה באמצעות ביטקוין[112].

סינגפור – הטילה לאחרונה חובה על כל השירותים הנוגעים למטבעות דיגיטליים להירשם ביחידה של המשטרה העוסקת במניעת הלבנת הון[113].

אוסטרליה – הרשות המופקדת על מלחמה בהלבנת הון, Austrac (Australian Transaction Reports and Analysis Centre), אוספת מידע על כל המרה של ביטקוין לדולר אוסטרלי וחזרה. איסוף המידע מתבצע לצורך זיהוי והתמודדות עם סיכונים בתחום הלבנת הון באמצעות ביטקוין[114]. כמו כן, מס רווחי הון חל על מכירת ביטקוין עד שנה מהקנייה. רווחים מכרייה יחויבו במע"מ. [115]

בארגנטינה, הרגולטור האחראי על הלבנת כספים פרסם הנחייה שכל טרנסאקציה שמבצע עסק באמצעות מטבע דיגיטלי צריכה להיות מדווחת לרגולטור.[116]

אקוודור אסרה על שימוש בביטקוין ובמטבעות דיגיטליים אחרים והחליטה להוציא לפועל מטבע דיגיטלי מדינתי. [117]

רגולציה בישראל

יחסן של הרשויות בישראל למטבעות דיגיטליים עדיין לא התגבש במלואו. לאחרונה (19.2.2014) פורסמה הודעה משותפת למספר גורמי ממשל ביניהם הרשות לניירות ערך בדבר הסיכונים הטמונים בשימוש, באחזקה ובהשקעה במטבעות דיגיטליים. ההזהרה התמקדה בסכנות הנובעות מהמעמד החוקי והרגולטורי המעורפל של מטבעות דיגיטליים, מכך שאינם מהווים הילך חוקי במדינה כלשהי, מהאפשרות לעשות בהם שימוש לצורך הלבנת הון ופעילויות לא חוקיות נוספות שנעשות באמצעותם או בהקשר אליהם. כמו כן, ההזהרה הציפה סכנות נוספות שנובעות מהתנודתיות בערכם של המטבעות הדיגיטליים עצמם, מחוסר היציבות והפיקוח הרופף על אתרים ושירותי מסחר וחלפנות המטפלים בהם ומהקושי לשמור עליהם מפני גניבה. זוהי הודעה רשמית ראשונה של הממשל הישראלי בנושא זה. יחד עם זאת, ההודעה נזהרה מלהגדיר את המטבעות הדיגיטליים בין אם כמטבעות (Currency), בין אם כסחורות (Commodity) ובין אם כניירות ערך (Security). כמו כן, ההודעה לא קבעה כל הנחיות מחייבות ספציפיות לגבי מיסוי, חשבונאות, ניהול סיכונים וכדומה.

---

[111] http://www.coindesk.com/government-backed-bitcoin-industry-association-launch-japan/

[112] http://virtualmining.com/canada-revenue-agency-says-tax-rules-apply-to-bitcoin/

[113] http://www.coindesk.com/bitcoin-regulation-roundup-bankruptcy-derivatives-consumer-protection/

[114] http://www.coindesk.com/australian-government-tracks-all-bitcoin-aud-conversions/

[115] http://www.coindesk.com/austria-offers-contradictory-guidance-bitcoins-financial-status/

[116] http://www.coindesk.com/argentinian-money-regulator-mandates-reporting-bitcoin-activity/

[117] http://www.coindesk.com/ecuador-bans-bitcoin-legislative-vote/

בניגוד למספר מדינות אחרות שכבר הודיעו לציבור באשר לחובות המס על שימוש במטבעות דיגיטליים, ישראל עדיין לא עשתה זאת. בינתיים, בחו"ד שהוזמנה על ידי ארגון הביטקוין הישראלי ממשרד רו"ח "שטיינמץ עמינח ושות"" נכתב כי אין חבות מס על רווחים אישיים מקנייה מזדמנת של ביטקוין ומכירתו בשער גבוה יותר בגלל הדמיון למסחר במט"ח[118]. כאמור, ההתייחסות הרגולטורית לביטקוין נמצאת בראשיתה ועדיין לא פורסמה הנחייה מחייבת מאף גורם רגולטורי, אם כי מספר גורמים מסרו שהם בוחנים את הנושא, לרבות בנק ישראל ורשות המיסים. בהמשך לכך, הוקם בבנק ישראל צוות בין משרדי שתפקידו לבחון את הנושא. הצוות כולל נציגים מרשות ניירות ערך, אגף שוק ההון, הביטוח והחיסכון במשרד האוצר, אגף החשב הכללי במשרד האוצר, משרד המשפטים, רשות המיסים, הרשות לאיסור הלבנת הון ובנק ישראל.

סיכום

תחום המטבעות הדיגיטליים טומן בחובו התקדמות טכנולוגית שעשויה להיות בעלת השפעה ניכרת על תחומי חיים מרכזיים בעולמנו, כגון אמצעי תשלום, מערכת הבנקאות, עולם ההשקעות הפיננסיות ועוד. בשלב מוקדם זה עדיין חלוקות הדעות באשר להתפתחות העתידית של התחום. יש הטוענים שהתפתחות הביטקוין ודומיו מסמנים מהפכה רחבת היקף בהתפתחות הכלכלה המודרנית, בעוד אחרים חוזים שמדובר בשלב ביניים בלבד ושעדיין אין באפשרותנו לחזות את ההשלכות של פיתוחים עתידיים שינבעו מטכנולוגיה זו. לאור חוסר ודאות זו, יתכן שמוטב לנהוג במטבעות הדיגיטליים במשנה זהירות.

תחום המטבעות הדיגיטליים הוא תחום חדש המעלה סוגיות מתחומי הטכנולוגיה, הכלכלה, המימון, המשפט, התרבות העסקית ועל כללי הזהירות בהם מחויבים לקוחות ומקבלי החלטות השקעה. הן הציבור והן הרגולטורים נדרשים ללמוד את הנושא על מנת לפעול באופן מושכל. מסמך זה, המהווה סקירה ראשונית בלבד, נועד לקדם מטרה זו באמצעות מתן סקירה כללית אודות מספר היבטים מרכזיים של מטבעות דיגיטליים, תוך התמקדות במטבע הדיגיטלי המוביל, ביטקוין. סקירה זו לא נועדה להוות תיאור ממצה של התחום ואף לא כדי להציג טענות באשר לאופן ההתנהלות הרצוי בהקשר למטבעות דיגיטליים. אלא, מטרתה הייתה להציג בצורה ברורה ככל שניתן את הטכנולוגיה, השימושים השונים והתגובות הרגולטוריות שהתהוו במהלך השנה האחרונה לביטקוין בפרט ולמטבעות דיגיטליים בכלל. זאת, על מנת לקדם את הידע הציבורי ואת הדיון הרגולטורי בנושא.

[118] http://www.bitcoin.org.il/files/חוות-דעת-מיסוי-ביטקוין.pdf

נספח 1: מתקפת העברה כפולה (Double Spending Attack)

נזכיר המרכיב השני של תהליך הווידוא[119], נועד למזער את ההסתברות שבלוק לא תקין יוכר על ידי שאר הכורים ויהפוך לחלק משרשרת הבלוקים הלגיטימית. כעת נניח שכורה מנסה לבצע את מה שקרוי מתקפת העברה כפולה. ההתקפה הטיפוסית תתבצע כך: הכורה ישקיע את כוח המחשוב שלו כדי לייצר שרשרת בלוקים בצורה סמויה (במחשבו האישי למשל). זו תהיה שרשרת בלוקים שיכולה להתחבר לשרשרת הקיימת וכוללת טרנסאקציות תקינות, אולם יש בה טרנסאקציה אחת שבה הוא שולח קבוצה מסוימת של מטבעות ביטקוין לעצמו במועד זמן T. במקביל הוא שולח הודעה פומבית שבה הוא יעביר את אותם מטבעות בדיוק לסוחר בתמורה למוצר כלשהו בזמן מאוחר יותר (T+1). הוא ימתין עד שהסוחר יעביר לו את המוצר ובינתיים ימשיך לעבוד על השרשרת הסמויה שלו בתקווה להצליח ולהפוך אותה לארוכה יותר מאשר סך הבלוקים שנוספו בינתיים לשרשרת הבלוקים המלאה. בשלב כלשהו הוא יפרסם את הבלוקים שלו. במצב זה ייוצר מזלג ברשת. שרשרת הבלוקים החל מנקודה מסוימת תתפצל בין שתי שרשראות מתחרות. הרשת בנויה כך שהשרשרת שתיחשב לאמתית היא זו הארוכה ביותר. לכן, אם התוקף הצליח לייצר אצלו שרשרת ארוכה יותר מכפי ששאר הכורים הצליחו לייצר בינתיים, ההתקפה שלו תצליח.

היכולת של התקפה כזו להצליח תלויה בכוח החישוב של התוקף, כלומר בקצב שבו הוא מייצר הוכחות עבודה (ראה נספח 2 למידע נוסף על הוכחות עבודה), ביחס לרשת כולה. אם הקצב שלו גבוה יותר משל שאר רשת הכורים, ההתקפה שלו תמיד תצליח. אבל יתכן שגם אם הקצב שלו נמוך יותר, הוא יצליח בכל זאת. משום שהזמן שלוקח למצוא פתרון הוא משתנה מקרי, עדיין יתכן שברגע כלשהו השרשרת של התוקף תהיה ארוכה יותר מזו של הרשת כולה ואם מצב כזה יקרה, ההתקפה תצליח. אולם, ברור שאם הקצב שלו נמוך יותר משל הרשת כולה, ככל שהסוחר ימתין ליותר אישורים (שיותר בלוקים יתווספו לרשת), כך היתרון של הרשת על פני התוקף יהיה גדול יותר, וכך יתמעט הסיכוי שהוא אי פעם יצליח לעקוף אותה. מני רוזנפלד, מראשי קהילת הביטקוין בישראל, חישב שהסיכוי להצלחה של התקפה כזו, כאשר הקצב של התוקף הוא 10% מהקצב של הרשת כולה מלבדו, וכאשר הסוחר ממתין ל-6 אישורים, יורדת מתחת ל 0.1%.[120] כוח המחשוב הנדרש כדי להגיע לקצב של 10% מהרשת הוא עצום ולכן יקר ביותר. מצב זה הופך את הניסיון לבצע מתקפות מהסוג הזה בעסקאות שאינן עסקאות ענק ללא כדאי. בעסקאות ענק ניתן להמתין למספר גדול יותר של אישורים.

כעת ניתן להבין מדוע כדאי למקבל הביטקוין להמתין לאישור לפני השלמת העסקה מהצד שלו (אספקת המוצר או מתן השירות). אישור הוא צירוף העסקה לשרשרת במסגרת בלוק. כל עוד העסקה אינה חלק מאף בלוק, תמיד יתכן שנותן הביטקוין נתן אותו במקביל לגורם אחר ואז אי אפשר לדעת איזו מהעסקאות תתקבל על ידי הרשת (בהנחה ששתיהן נשלחו בו זמנית). אולם, ברגע שהתקבל אישור אחד על העסקה, כלומר, היא צורפה לשרשרת, ההסתברות שהתבצעה עסקה סותרת ושעסקה זו תתקבל על ידי הרשת יורדת בצורה תלולה.

זמן ההמתנה לאישור תלוי במועד שבו העסקה המדוברת תצורף על ידי כורים לבלוק. זמן זה עומד עבור טרנסאקציה ממוצעת על כעשר דקות בממוצע. על מנת להבטיח שהטרנסאקציה שלו תקבל עדיפות, יכול המשתמש לשלם עמלה. העמלה תתקבל אצל הכורה שיוסיף את הבלוק שיכלול את העסקה ולכן כורים יעדיפו לצרף עסקה זו על פני אחרות והיא תאושר מהר יותר.

---

[119] המרכיב השני של התהליך הוא שכחלק מתהליך צירוף הבלוק לשרשרת הבלוקים, נדרש כל כורה לאשר את כל הבלוקים הקיימים בשרשרת שאליה הוא רוצה לצרף את הבלוק שלו. האישור כרוך בבדיקה שכל הבלוקים בשרשרת תקינים. בלוק תקין הוא בלוק שלא כולל טרנסאקציות סותרות ושבו לכל ביטקוין יש היסטוריה תקינה.

[120] https://bitcoil.co.il/Doublespend.pdf

נספח 2: פונקציית הגיבוב (Hash Function)

כעת נתאר בקצרה את אותה בעיה מתמטית שנדרשים הכורים לפתור. הבעיה היא מציאת פתרון לפונקציה מסוג פונקציית גיבוב (hash function). פונקציית גיבוב היא כל פונקציה שמקבלת מידע באורך אקראי ונותנת כתוצאה מידע באורך קבוע. בפרוטוקול הביטקוין, הבעיה היא מציאת n, כאשר n הוא פרמטר בפונקציה, כך שהתוצאה של פונקציית הגיבוב תהיה נמוכה מ-a. ברור שככל ש-a נמוך יותר, קשה יותר למצוא את n. תכונה זו מאפשרת לפרוטוקול להתאים את a בהתאם לכוח המחשוב של רשת הכורים כך שייקח בממוצע עשר דקות כדי למצוא את הפתרון. כך, a משמש כפרמטר הקובע את רמת הקושי של מציאת הפתרון. תכונה חשובה נוספת של פונקציית גיבוב היא האסימטריה שלה. כלומר, קשה מאוד למצוא פתרון לפונקציה, אבל קל מאוד לאשר אם פתרון מוצע כלשהו הוא נכון או לא נכון. קלות זו מאפשרת לכורים לאשר מחדש את כל הבלוקים הקיימים בכל הוספת בלוק חדש בלי לבזבז על כך משאבים רבים מדי.

נספח 3: "גמישות עסקאות" (Transaction malleability)

גמישות עסקאות היא חולשה זניחה למדי במערכת ביטקוין שלמרות זאת יכולה לשמש להתקפות מול מערכות תשלומים פגומות, ולאחרונה נטען שהיא גרמה לקריסה של עסקים רבים בתחום הביטקוין, כמו ל- MtGox, שהייתה עד אז הבורסה המובילה בעולם למטבעות דיגיטליים.

לצורך פשטות ניתן לתאר עסקה פשוטה בביטקוין כמכילה את המידע הבא: "דני נותן לדינה 100 ביטקוין". בנוסף, העסקה כוללת חתימה אלקטרונית שמטרתה להבטיח שכל פרטי המידע הללו לא ישתנו. כלומר, שינוי הנותן, שינוי המקבל או שינוי הסכום, כל אחד מהם יהפוך את החתימה לבלתי קבילה ורשת הכורים תדחה את העסקה. בנוסף לכל אלה, העסקה כוללת גם מספר סידורי. המספר הסידורי הזה ניתן לשינוי בלי לפגום בחתימה. ניתן להשתמש בפרט זה על מנת לרמות משתמש או מערכת תשלומים המשתמשת במספר הסידורי בלבד על מנת לעקוב אחרי תשלומים.

לדוגמא, נניח שדינה רוצה לרמות את דני. דני משדר את הודעתו "דני נותן לדינה 100 ביטקוין", הודעה זו חתומה ומקבלת את המספר הסידורי 700. דינה, גם היא שייכת לרשת הכורים והיא מקבלת הודעה זו, משנה את המספר הסידורי ל-7001 באמצעות הוספת הספרה 1, בסוף המספר הסידורי המקורי, ומיד משדרת אותה לרשת הכורים. אם העסקה של דינה מצטרפת לבלוק לפני העסקה של דני, העסקה של דני תידחה משום שקיימת כבר עסקה זהה. אולם, אם שירות הארנק של דני בודק אם העסקה שלו אושרה לפי המספר הסידורי בלבד, הוא לעולם לא ילמד על ביצוע העסקה. מצב זה יכול להוביל לכמה השלכות: ראשית, יתכן שדני יבצע את העסקה שוב ואז דינה תקבל 200 ביטקוין במקום 100; שנית, אם דני משתמש במערכת תשלומים אוטומטית, יתכן שהמערכת תמשיך לשלוח עסקאות כל עוד העסקאות לא מתקבלות. כך יתכן שדני יאבד הרבה יותר מה-100 ביטקוין שהוא התכוון לשלם. כמובן שמערכת תשלומים אינטליגנטית קצת יותר לא תהיה פגיעה לסוג כזה של רמייה.