digital whisper
Technologic Papers

שימוש בטוח בביטקוין מהסוף להתחלה

מאת יוני יחזקאל

הקדמה

ביטקוין, המטבע הדיגיטלי המבוזר שצבר כותרות בשנה האחרונה ובייחוד בחודש האחרון כאשר ערכו עבר את ה-$1000 ל"יחידה", הולך וצובר משתמשים. אחד היתרונות הגדולים של הביטקוין על פני מטבעות אחרים הוא הניהול המבוזר שלו ועל כן היכולת של כל אחד לנהל בעצמו את ארנק (חשבון) הביטקוין שלו ללא צורך בבנק או בכל צד ג' נוסף. קיימים כיום שירותים המציעים לנהל עבור המשתמשים את ארנק הביטקוין שלהם, אך מרביתם אינם מספקים אחריות במקרה של אובדן או גניבה, אפילו אם מדובר בתקלה או בפרצה אצל נותני השירות. לאחרונה נגנבו מארנקי אונליין כאלה ואחרים אלפי בטקויינים בשווי כמה מיליוני דולרים[1]. יכולת הניהול העצמית של הביטקוין, חוסר האחריות ובהרבה פעמים גם חוסר הכשירות של ספקי השירות הקיימים היא הסיבה שרבים ממחזיקי המטבע מעדיפים לנהל את הארנקים שלהם בעצמם ולא לסמוך על צד שלישי שינהל אותו.

בתחילת דרכו של המטבע, הרוב המוחלט של המשתמשים בו היו חובבי קריפטוגרפיה ומחשבים, אך היום מחזיקים במטבע מספר רב של אנשים ללא רקע טכני ויש צורך באמצעי אבטחה שיהיו חזקים מספיק כדי לשמור את הארנקים בטוחים אך מצד שני פשוטים כדי שגם המשתמש הממוצע יוכל להשתמש בהם.

במאמר זה נסקור את הדרכים בהן ניתן לאבטח ארנק ביטקוין מפני אובדן וגניבה. בסיומו נתייחס לעוד שני נושאים שחשובים גם הם בשימוש יומיומי ונרחב של ביטקוין - הגנה מפני רמאויות, ושמירה על פרטיות. במאמר נניח שרוב הקוראים מתמצאים באבטחת מידע ברמה זו או אחרת ועל כן לא נכנס לפרטים בנושאים בסיסיים כמו ניהול סיסמאות, זיהוי בשני שלבים, הצפנה, האשינג, ונושאים אחרים שכמובן חשובים מאוד כדי ליצור ארנק מאובטח אך אינם קשורים ספציפית לביטקוין. כמו כן, לא נדבר בכלל על פרוטוקול הביטקוין עצמו ובעיות אבטחה שעלולות להתקיים בו ונניח כי מערכת הביטקוין עצמה פועלת בצורה תקינה ובטוחה.

[1] http://www.wired.com/wiredenterprise/2013/11/inputs

כמה מילים על ארנק ביטקוין

ארנק ביטקוין מורכב מאוסף של כתובות ביטקוין וזוג מפתחות עבור כל כתובת מפתח פרטי ומפתח ציבורי. בקצרה נזכיר שכתובת הביטקוין היא בעצם ההאש של המפתח הציבורי. בעת ביצוע העסקה משמש המפתח הפרטי לחתום עסקאות שמעבירות כספים מהכתובת המקושרת למפתח הפרטי לכל כתובת אחרת. בשום שלב המפתח הפרטי אינו נשלח ברשת והמידע היחיד שיוצא בפועל מהמחשב של המשתמש ונשלח בין הצמתים המפעילים את רשת הביטקוין הוא תיעוד העסקה החתומה במפתח.

[כתובת ביטקוין שנוצרה בעזרת האתר bitaddress.org]

במידה והעסקה חתומה בצורה תקינה, ונשלחים הביטקוינים הנמצאים ברשותו של השולח, היא בסופו של דבר תרשם בבלוק ותכנס לעד לבלוקצ'יין[2] (מאגר המידע המשותף בין כל הצמתים ברשת הביטקוין). כאשר אנו מדברים על אבטחה של "חשבון" ביטקוין אנחנו בעצם מדברים על הדרך בה נוכל לשמור את המפתח הפרטי זמין לשימוש שלנו אך מוגן מגניבה או אובדן.

אבטחת ארנק

ארנק חומרה

[ארנק חומרה של חברת trezor]

ארנקי חומרה הם המילה האחרונה באבטחה ושימוש בביטקוין. ארנק חומרה שומר את המפתח הפרטי אצלו בדרך שאינה ניתנת לשליפה. הארנק מתחבר ב-USB או bluetooth למחשב או לפאלפון. כאשר המשתמש מעוניין לבצע עסקה פרטי העסקה נשלחים לארנק החומרה. הארנק חותם את העסקה ושולח חזרה את העסקה החתומה. בגלל שאין דרך להוציא את המפתח הפרטי מהארנק אך עדיין ניתן להשתמש בו בקלות באופן שוטף הוא נחשב לאחת הדרכים הנוחות והבטוחות להשתמש בביטקוין.

[2] https://en.bitcoin.it/wiki/Block_chain

חשוב מאוד שלארנק החומרה יהיה מסך בו הוא יכול להציג למשתמש את פרטי העסקה שהוא מאשר כך שלא יווצר מצב בו הפלאפון או המחשב מציג למשתמש עסקה אחת אבל בפועל המשתמש מאשר עסקה אחרת. כמו כן המסך יכול לשמש להצגת המפתח הפרטי בצורה בטוחה לשם גיבוי שלו על ידי המשתמש. ארנקי חומרה מתוחכמים מעט יותר יכולים גם להכיל מקלדת קטנה ולדרוש קוד כדי לבצע חתימה על עסקה דבר שמגן על השימוש בהם במקרה של גניבה פיזית ואפילו להכיל בתוכם רכיבי תקשורת GSM ו-Wifi המאפשר להם לבצע טראנסקציות עצמאית ללא צורך בחיבור למכשיר מתווך.

חסרונו העיקרי של ארנק חומרה הוא שעדיין מדובר ברכיב אלקטרוני שעלול להיכשל בשלב כזה או אחר ועל כן יש חשיבות מירבית בשמירה על גיבוי במקום בטוח. הדרך המומלצת לבצע גיבוי לארנק החומרה היא באמצעות ארנק נייר עליו נדבר בהמשך. לצערנו, מרבית ארנקי החומרה נמצאים עדיין בשלב האבטיפוס ואינם זמינים לרכישה ושימוש (אם כי גרסאות ראשונות של המכשירים הללו אמורים להיות זמינים בחודשים הקרובים). כך שנכון לעכשיו משתמשי הביטקוין צריכים לחשוב על פתרונות אחרים לשמירה על הארנקים שלהם.

ארנק נייר

שימוש בארנק נייר היא הדרך הקלה והבטוחה לשמור כתובת ביטקוין, אם כי היא עלולה להיות מעט מסורבלת. במקום לשמור את המפתחות בצורה דיגיטלית על המחשב, המפתח מודפס על דף נייר (ארנק זה מכונה גם הרבה פעמים אחסון אופליין או אחסון קר). לאחר תהליך יצירת המפתחות והכתובת המשתמש יכול להעביר את הכתובת לכל מי שהוא מעוניין ולהמשיך לקבל תשלומים. שירותים מסויימים כמו blockchain.info והגרסה הבאה של bitcoinQT מאפשרים למשתמשים לצפות ולקבל עידכונים על המאזן של כתובת מסויימת ללא צורך במפתח הפרטי שלה.

[כתובת נייר שנוצרה בעזרת האתר bitaddress.org]

מעבר ליתרון האבטחה בשמירה של מפתחות אופליין, ניירות הן צורת אחסון אמינה הרבה יותר מרכיבים אלקטרונים. כל עוד לא יהיה חשוף לנזקי אש או מים, המידע על דף נייר יכול להישמר בקלות לעשרות שנים הרבה אחרי שכל מצע אלקטרוני יסיים את חייו.

לעומת זאת, קיימים לארנקי נייר מספר גם חסרונות:

- **יצירת הכתובות חייבת להתבצע בסביבה סטרילית ובטוחה לחלוטין:**

יצירת סביבה סטרילית לחלוטין היא משימה לא קלה ויש שיגידו בלתי אפשרית. במחשב הממוצע מותקנות תוכנות זדוניות כאלה ואחרות. ובעוד שחוקר אבטחה אולי יכול לסמוך על סביבת העבודה שלו יותר מהמשתמש הממוצע, ניתן להניח שדווקא מי שמודע לסכנות האפשריות לא ירצה להשאיר יותר מידי פתח לסיכונים.

ההסכמה הגורפת היא שבשביל ליצור ארנק נייר מומלץ להשתמש במחשב ייעודי למטרה זו, מחשב שלא מחובר לרשת וגם לא יהיה מחובר אליה בעתיד. ישנן אף מדפסות ייעודיות כמו ה-Piper אשר יכולות להדפיס כתובות ביטקוין עצמאית ללא צורך בחיבור למחשב או לרשת. למרות המחירים האטרקטיבם של מחשבים בימינו עדיין למעטים ישנו מחשב ייעודי או מדפסת הזמינים אך ורק בשביל יצור כתובות ביטקוין. ולכן למי שאין ברשותו מחשב ייעודי ההמלצה היא להשתמש ב-liveCD של הפצת לינוקס כזו או אחרת כדי לייצר את הכתובות. בעת הייצור על המחשב להיות מנותק לחלוטין מהרשת ויש לכבות אותו מיידית לאחר הדפסת הכתובות. כמובן שגם כאן עלולים להיות סיכונים.

מדפסות רבות היום מחוברות בעצמן לרשת וחלקן אף שומרות העתקים של הדפים המודפסים באחסון פנימי. ועל כן חשוב שהמדפסת עצמה תהיה מדפסת "טיפשה" אשר אינה מחוברת לרשת בעת ההדפסה. כמו כן גירסת ה-LiveCD עצמה בה משתמשים עלולה להכיל מראש רכיב זדוני או שהביוס עצמו עלול להיות נגוע בנוזקה כזו או אחרת שיוכלו לשמור את המפתחות במחשב המשתמש ולשלוח אותן בעתיד כאשר הוא יחובר מחדש לרשת. נכון לעכשיו לא נראה שקיימות בשטח נוזקות עם היכולות האלה, אבל ניתן לשער שבעתיד עם העליה בשימוש ובערך של הביטקוין יימצאו גם מי שיכתבו וינסו להפיץ נוזקות כאלה.

[מדפסת פייפר וכתובת נייר שהודפסה בעזרתה]

- **ארנק נייר הוא חד פעמי:**

ניתן להפקיד מטבעות לאותו ארנק נייר מספר פעמים. אך כאשר אנו מעוניינים למשוך כספים מהחשבון עלינו להשתמש במפתח כדי לחתום את העסקה. שלב החתימה עצמו אינו דורש חיבור לרשת אך יצירת העסקה והשליחה שלה כן דורשים חיבור. לרוב המשתמשים יהיה קשה ומסורבל להפריד בין השלבים (למרות שישנן תוכנות ארנק כדוגמת Armory המאפשרות לייצר עסקאות על מחשב אחד ולחתום אותן על מחשב אחר), ולכן בתהליך זה המפתח עלול להיחשף ולא יהיה בטוח להשתמש בו שנית. הדרך הפשוטה ביותר להתגבר על החסרון הזה היא לייצר מראש מספר רב של כתובות בארנק נייר וכאשר משתמשים בכתובת אחת להעביר את היתרה שנשארה בה לכתובת הבאה (גם כאשר משתמשים בארנק חם אשר אינו אופליין שימוש נכון בביטקוין ממליץ לא להשתמש באותה כתובת יותר מפעם אחת ותמיד להעביר את היתרה לכתובת חדשה).

- **ארנק נייר חשוף לגניבה ופגיעה פיזית:**

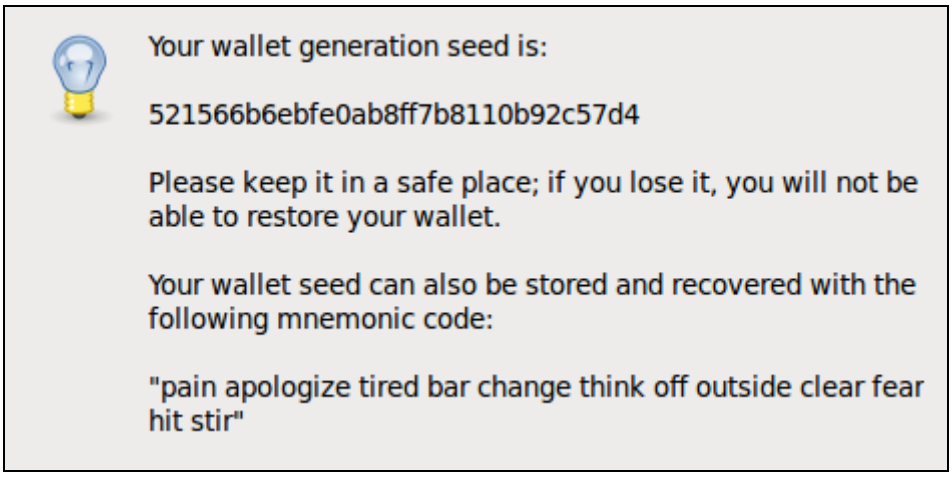
חשוב לזכור שלמרות רמת האבטחה הגבוהה שיש לנו בשימוש בארנק נייר מפני פריצות דיגטליות. במידה ומישהו יפרוץ לנו פיזית לבית או יעשה לנו חיפוש עם צו בדירה, הוא יוכל לקחת מאיתנו את המפתחות הפרטיים. כמובן שניתן לשמור את דפי הנייר עצמם בכספת בבית או בבנק אבל בדומה למחשב נקי האופציה הזו לא זמינה בפני רוב המשתמשים. למרות שהסיכוי לפריצה פיזית קטן משמעותית מהסיכוי לפריצה למחשב עדיין נרצה להיות בטוחים גם ממנה. ועל כן ניתן לשמור את המפתח הפרטי על הנייר בצורה מוצפנת עם סיסמא (אותה כמובן חשוב לזכור!). אבל גם הסיסמא ואולי אפילו הכספת לא יעזרו לנו אם מחר השכנים שלנו ישכחו את התנור דולק בלילה וכל הבניין יעלה באש. לכן מומלץ כמובן להדפיס שני העתקים ועותק אחד לשמור אצל חברים או קרובי משפחה. מי שרוצה להשקיע קצת יותר יכול לפצל את המפתחות למספר גורמים עם השיטה שפיתח עדי שמיר המאפשרת לקחת חתיכת מידע ולפצל אותה למספר גורמים כך שהמידע גם מוגן מגניבה אך עדיין זמין לשיחזור אם אחד החלקים אובד[3]. לא נפרט על הטכניקה כאן אבל מי שלא מכיר אותה מוזמן לקרוא עליה עוד בקישורים.

למרות החסרונות והסרבול הנדרש ביצירת ארנק נייר, זו השיטה המומלצת לשמירת גיבוי לכתובות ביטקוין. לא משנה באיזו שיטה נוספת נשתמש בכדי לייצר את הארנק שלנו תמיד מומלץ בנוסף לגבות אותו גם בצורה פיזית. 95% מהמקרים של אובדן ביטקוין היא על ידי משתמשים שאבדו את הסיסמה לארנק שלהם ולא היה להם גיבוי על נייר.

[3] http://en.wikipedia.org/wiki/Shamir's_Secret_Sharing

- **ארנק מוח \ ארנק דטרמיניסטי:**

שימוש בארנק מוח היא שיטה מאוד קלה ובטוחה, אך היא סומכת לחלוטין על זכרונו של המשתמש. ארנק מוח הוא בסופו של דבר סיסמא, רק שבמקום להשתמש בסיסמא על מנת לפתוח מידע מוצפן או לגשת לשירות מסויים, הסיסמא מתוגרמת ישירות למפתח פרטי באמצעות האשינג עם SHA256. ארנק דטרמיניסטי בדומה לארנק מוח זקוק רק לסיסמא בכדי לשחזר את הארנק אבל בשיטה זו מחושב מהסיסמה seed היכול לשמש ליצירה של מספר אינסופי של כתובות במקום כתובת אחת. החסרון העיקרי בשיטות אלה הוא שעל המשתמש לבחור סיסמא חזקה מאוד שתהיה עמידה לברוטפורס ברמות הגבוהות ביותר. מומלץ שהסיסמא תהיה מורכבת מעשרות תווים ולא תכיל משפטים מוכרים. תוכנת Electrum מאפשרות לקבל גיבוי של ה-seed כסיסמא המורכבת מ-12 מילים ובכך מייעלת את תהליך בחירת הסיסמא.



[גיבוי דטרמיניסטי לארנק של תוכנת Electrum]

בדומה לארנק נייר יש צורך בסביבה סטרלית בעת היצירה של הכתובת הראשונית. ובמידה ורוצים למשוך את הביטקוין יש צורך לעשות זאת גם כן בסביבה סטרלית או להתייחס לכתובת כחד פעמית. אם מדובר בארנק דטרמיניסטי נעדיף כמובן לחשוף רק את המפתח הפרטי של כתובת יחידה ולא את הסיסמא כולה במידה והדבר אפשרי.

חסרון נוסף של ארנק מוח הוא שבמידה ובעל הארנק שוכח את הסיסמא, או חס וחלילה נפגע שכלית ואולי אף נפטר בצורה פתאומית ולא נשמר גיבוי בשום צורה אחרת הביטקוין שלו אבדו לנצח. מומלץ להשתמש בארנק מוח רק על ידי מי שמבין את הסיכונים בצורה מלאה ויודע לבחור סיסמאות חזקות בצורה מתאימה. גם אז מומלץ תמיד לגבות את הארנק בצורה נוספת. הסיבה היחידה אולי להשתמש בארנק מוח בלבד ללא גיבוי היא כאשר אנו רוצים להגן על עצמנו באופן מוחלט מפני החרמה של הביטקוין על ידי רשויות החוק. אבל כל עוד אנחנו פועלים במסגרת החוק קשה להאמין שיש סיבה שלא לשמור גיבוי נוסף.

- **ארנק תוכנה \ ארנק אונליין:**

ארנקים אלה מכונים גם ארנקים חמים. ארנקים אלה מאוד קלים ליצירה ושימוש יומיומי. ההבדל העיקרי בין ארנק תוכנה המותקן במחשב לבין ארנק אונליין הוא שבארנק תוכנה כל המידע נשמר על מחשב המשתמש ואילו בארנק אונליין המידע נשמר בשרתים של החברה שמספקת את השירות. במידה וניתן לסמוך על החברה המספקת את הארנק רמת האבטחה של ארנק אונליין יכולה להיות דומה ולפעמים אפילו גבוהה יותר מרמת האבטחה של ארנק מקומי.

כדי להשתמש בארנק תוכנה כל שצריך הוא להתקין את אחת מתוכנות הארנק הזמינות על המחשב. בעת ההפעלה התוכנה תייצר מספר כתובות לשימוש מיידי. מכיוון שכל המפתחות זמינים ישירות לתוכנה, כל מה שהמשתמש צריך לעשות הוא להשתמש בתוכנה להעברת כספים או לקבל ממנה כתובת אליה יכולים לשלוח לו כספים. ניהול המפתחות הפרטיים ויצירה של כתובות חדשות נעשה בצורה כמעט שקופה לחלוטין מבחינת המשתמש.

למרות שניתן ואף מומלץ להצפין את המפתחות ולגבות אותם הדבר לא קורה כברירת מחדל ועל המשתמש להיות מודע לאפשרויות האלה. יותר מזה, מכיוון שארנקי תוכנה יוצרים כתובות חדשות בעת השימוש בהן (בעיקר בעת שליחה של כספים) מומלץ לגבות את הארנק מחדש לאחר ביצוע פעולות.

ארנקי אונליין קלים אף יותר לשימוש מארנקי תוכנה מכיוון שהמשתמש אינו צריך אפילו להתקין תוכנה על המחשב. ברוב המקרים ארנקי אונליין יקחו על עצמם הן את משימת הגיבוי והן את משימת האבטחה של הארנק ויחסכו מהמשתמש לבצע את הפעולות האלה בצורה ידנית.

על ארנקי אונליין קשה לדבר כמכלול שלם מכיוון שישנו מספר רב של שירותי אונליין המציעים שמירה של הביטקוין עבור המשתמשים וכל יום צצים שירותים חדשים. לצערנו ישנם שירותים רבים אשר אינם מבינים באבטחת מידע ויותר מזה עלולים בעצמם לגנוב את המטבעות המופקדים בהם ולכן חשוב מאוד להשתמש בשירות מוכר ואמין ולהבין כיצד הוא עובד. מכאן והלאה נדבר רק על שירותי צד שלישי שנחשבים לאמינים. ישנם שני סוגים עיקריים של ארנקי אונליין הראשון כדוגמת coinbase מנהל בצורה מוחלטת את הביטקוין של המשתמשים בו. השירות כלל לא שומר את הביטקויינס של כל לקוח בנפרד וכל המטבעות נשמרים בחשבונות בשליטת החברה. לטענת מפעילי האתר בפועל 90% מהמטבעות שלהם נשמרים בכלל באחסון קר על ארנקי נייר השמורים בכספות במספר מוקדים. פורץ שיפרוץ לשרתי coinbase ויגנוב משם את 10%הביטקוינים שכן שמורים בארנקים חמים, לא יגנוב בפועל ביטקוינים מהמשתמשים אלא מהחברה עצמה. מעניין יהיה לראות כיצד תגיב החברה לכך וכמה מנזקי הפירצה יגולגולו חזרה למשתמשים. מה שברור הוא שבמקרים קודמים בהם נפרצו חשבונות ספציפיים של משתמשים ונגנבו מהם מטבעות החברה לא פיצתה את המשתמשים לאחר

מכן. כך שעל המשתמשים לדאוג לאבטח את החשבונות שלהם בצורה הולמת (סיסמא חזקה, זיהוי בשני שלבים) וכן את המחשבים בהם הם משתמשים לגשת לשירות. במידה ושירות coinbase יסגר למשתמשים לא תהיה שום יכולת לגשת למטבעות שהופקדו שם.

הסוג השני של ארנק אונליין הוא ארנק היברידי, כדוגמת blockchain.info, המשתמש בשרתיו אך ורק כגיבוי מוצפן למפתחות הפרטיים. גם אם שרתי החברה נפרצים כל המפתחות מוצפנים ולא ניתנים לשחזור ללא סיסמת המשתמש. כל תהליך ההצפנה והפתיחה של הארנק מתבצע בדפדפן והסיסמה מעולם לא נשמרת או אפילו נשלחת לשרתי החברה. אם השירות נסגר ומפסיק לפעול המשתמש עדיין יכול להשתמש בגיבוי שנשמר אצלו מקומית כדי למשוך את הביטקוין מהארנק שלו ללא צורך בשיתוף פעולה מצד מפעילי השירות. בהנחה שהמשתמש בחר בסיסמא חזקה (ומומלץ גם להשתמש בזיהוי 2 שלבים) הוא יכול להיות בטוח שגם אם שרתי החברה יפרצו או רשויות החוק יבקשו גישה למטבעות שלו המטבעות שלו עדיין יהיו בטוחים כי לא ניתן להשתמש במידע השמור על שרתי החברה ללא הסיסמה. מכיוון שאם שרתי החברה יפרצו ביכולתו של הפורץ לשנות את קוד האתר כך שישלח את הסיסמא לשרת ולשמור אותה שם מומלץ להשתמש בתוסף לדפדפן המריץ העתק של האתר בצורה מקומית ולא סומך על קוד המגיע מהשרת כלל. משתמש אשר ישתמש בכל אמצעי האבטחה העומדים לרשותו עם ארנק מסוג זה יוכל להגיע לרמת אבטחה הכמעט זהה לזו של ארנק תוכנה מקומי. בנוסף יזכה לגיבויים אוטומטים וכן להצפנה הכרחית כך שלמשתמש הפשוט ארנק אונליין מסוג זה יהיה מוגן יותר מארנק היושב מקומית במחשב ולא עובר גיבוי והצפנה, אך בסופו של דבר גם ארנקים אלה בטוחים רק כל עוד המחשב בו משתמשים בהם בטוח.

- **ארנק פלאפון:**

ארנק פלאפון הוא הדרך הזמינה ביותר להשתמש בביטקוין. במדינות רבות בעולם ואפילו בישראל ישנם עסקים מקומיים המקבלים ביטקוין. הדרך הנוחה אם לא היחידה היום לשלם בעסקים אלה היא באמצעות תוכנות ארנק המותקנות על הפלאפון. בדומה למחשב גם לפלאפון ישנן תוכנות ארנק המותקנות על המכשיר ותוכנות הזמינות אונליין. רמת האבטחה של ארנקים אלה דומה לארנקים המשתמשים בהם במחשב כאשר ההבדל העיקרי הוא שסביבת הריצה בפלאפונים באופן כללי נחשבת להרבה פחות בטוחה מסביבת הריצה במחשב. כמו כן, ישנה סכנה הרבה יותר גדולה שהפלאפון יגנב יאבד או יתקלקל ועל כן חשוב מאוד לשמור על גיבוי לארנק. באופן כללי אם אנחנו מסתכלים על ארנק נייר כמקביל לכספת בבנק אנחנו צריכים להסתכל על ארנק בפלאפון כמקביל לארנק אותו אנחנו סוחבים בכיס כל הזמן ולדעת שקיים סיכוי שהוא יגנב או יאבד..

מהסקירה שעשינו על מגוון השיטות לשמור על כתובת ביטקוין ניתן להבין שאין שיטה אחת שניתן להשתמש בה. ארנקי נייר אולי מאוד בטוחים מפני אובדן או גניבה אבל קשים לשימוש יומיומי. ואם נרצה להשתמש בביטקוין שלנו לשלם על בירה בפאב השכונתי כנראה שנהיה חייבים להסתובב עם תוכנת ארנק שתהיה מותקנת בטלפון. ועל כן הדרך הבטוחה והשימושית ביותר להשתמש בביטקוין היא בשילוב של מספר ארנקים:

- ארנקי נייר לחסכונות ביטקוין האמורים להשמר לזמן רב וכן כגיבוי לכל שאר הארנקים שלנו.
- ארנקי תוכנה \ ארנקי אונליין לסכומים קטנים לקניות אונליין ושימוש יומיומי.
- ארנק בפלאפון לסכומים קטנים עוד יותר לשימוש יומיומי מיידי.

כניסה של ארנקי חומרה לשוק ושימוש נרחב בהם יוכל להקל על האבטחה והשימוש היומיומי בביטקוין אבל גם אותם כנראה שנרצה לגבות על ארנק נייר.

מניעת רמאויות

ביטקוין הוא מטבע מבוזר השואף להיות דומה למזומן דיגטלי. לאחר ביצוע העברה לא ניתן לבטל את העברה במקרה של רמאות או אי-קבלת המוצר. לכן יש לשים לב - כאשר מבצעים רכישה בביטקוין חשוב לדעת שניתן לסמוך על המוכר לספק את הסחורה. אתרי מסחר רבים המשתמשים כמתווכים בין המוכר לקונה מספקים שירותי ESCROW בהם הכספים נשמרים אצל האתר המתווך עד שהלקוח מאשר את קבלת המוצר. הבעיה בשירותים אלה היא שבמידה והגורם המתווך נסגר או מחליט להעלם עם הכסף שהופקד אצלו ללקוחות ולעסקים אין דרך לקבל את הביטקוינים שלהם בחזרה.

פתרון לבעייתיות בשימוש ב-ESCROW הוא שימוש בכתובת מרובות חתימה. כתובות ביטקוין אלה מאפשרות למשוך מהן כספים אך ורק באישור החתום על ידי מספר מפתחות פרטיים (ניתן להגדיר סף של m מ-n). מוכר וקונה יכולים לייצר כתובת כזו במשותף עם צד ג' ששניהם סומכים עליו. הקונה יעביר אליה את סכום הרכישה. לאחר קבלת המוצר, יאשרו הן המוכר והן הקונה העברה המעבירה את הכסף מהכתובת המשותפת לכתובת שברשות המוכר בלבד. במידה ולא תהיה הסכמה יוכל כל אחד מהצדדים לפנות לגורם המתווך הנבחר ולבקש ממנו לחתום איתם על העברה של הכסף. הגורם המתווך אינו יכול למשוך את הכספים בעצמו ללא שיתוף פעולה של אחד הצדדים ואם שני הצדדים פועלים בצורה הוגנת ומסכימים בניהם הם אינם זקוקים כלל לשיתוף פעולה מצד הגורם המתווך.

למרות שכתובות מרובות חתימה מוגדרות ונתמכות על ידי פרוטוקול הביטקוין אין כיום תוכנות ארנק נפוצות המאפשרות ליצור ולהשתמש בכתובות כאלה אך ניתן לשער שאם תהיה לכך דרישה רבה מצד המשתמשים ארנקים רבים יתחילו לממש את החלק הזה של הפרוטוקול.

פרטיות

למרות ההצהרות הרבות בתקשורת על השימוש בביטקוין בידי ארגוני פשע והאנונימיות בשימוש בו הדבר רחוק מלהיות נכון. חשוב לזכור כי הבלוקצ'יין ובו כל עסקאות הביטקוין זמין לעיון על ידי כל מי שמעוניין בכך. אומנם אין קישור בין כתובת מסויימת לבעלי הכתובת אבל במידה וישנה דרך לקשר בין הכתובת לבעל החשבון (נגיד במידה והוא פרסם אותה באתר האינטרנט שלו) ניתן לגלות את כל ההעברות שהגיעו לכתובת זו ונשלחו ממנה. יותר מזאת אם התבצעה העברה מכתובת זו הכוללת שימוש בכספים מכתובות נוספות (כפי שמתאפשר בפרוטוקול ומתבצע אוטומטית על ידי מרבית תוכנות הארנק), ניתן לשער כמעט בוודאות כי כל הכתובות שייכות לאותה יישות ואף נעשו נסיונות לקשר בין כלל הכתובות בבלוק ציין ליישויות המחזיקות אותן[4]. ארגוני פשע מנוסים בהעלמת כספים ושימוש באנשי קש גם בכסף שאינו דיגיטלי אך לאדם הפשוט יהיה הרבה יותר קשה לקבל מראש כספים בביטקוין מבלי לחשוף את הזהות שלו.

כדי לשפר מעט יותר את האנונימיות של ביטקוין מוצעים היום מספר שירותי "מכבסה" המשמשים להלבנה של ביטקוין. המשתמש שולח את המטבעות שלו לכתובת של השירות ומשם הם מתערבבים לעשרות כתובות ביטקוין עם מטבעות של לקוחות אחרים. מעשרות כתובות אחרות נשלחים מטבעות בסכום דומה לכתובת חדשה של המשתמש. ככה כל אחד מקבל כסף של מישהו אחר ורק נותני השירות יכולים לדעת למי שייך הכסף.

הבעיה גם פה היא בהסתמכות על צד שלישי שיכול גם לגנוב את הכסף וגם לחשוף את זהות המשתמשים או לפחות את הכתובות המקוריות של המשתמשים בשירות. כיום מפותח פרוטוקול zerocoin הפועל על גבי רשת הביטקוין ויאפשר לצמתי ביטקוין המעוניינים בכך להפעיל שרותי מכבסה מבוזרים שיהיו אנונומיים לחלוטין.

בנוסף חשוב לדעת כי למרות שכתובת ה-IP של המשתמש לא נרשמת בבלוקצ'יין הצמתים המקבלים אליהם את ביצוע העסקה יודעים מי הצומת ממנה הם קיבלו אותה. ממשלה או גוף גדול יכול להפעיל מספר צמתי ביטקוין ברחבי העולם ובכך לזהות כמעט במדיוק מה כתובת ה-IP של המחשב שיצר את

[4] http://eprint.iacr.org/2012/584.pdf

העסקה. לכן מי שרוצה לשמור על אנונימיות גבוהה מומלץ שישתמש ב-TOR או ב-VPN אנונימי בכדי לבצע את הטראנסקציות.

על כותב המאמר

יוני יחזקאל - מהנדס תוכנה המתמחה בפיתוח פרונט אנד וטכנלוגיות ווב. חובב אבטחת מידע, קוד פתוח וביטקוין. תוכלו למצוא עוד מידע וכלים כמו LiveCD המיועד לייצור ארנקי נייר ושימוש ביטקוין בבלוג שלי ב:

https://blog.non.co.il

תודות

תודה למני רוזנפלד מאיגוד הביטקוין הישראלי על העזרה בכתיבת המאמר.

לקריאה נוספת

- https://en.bitcoin.it/wiki/Securing_your_wallet
- http://bitcoin.org/en/secure-your-wallet
- https://en.bitcoin.it/wiki/Hardware_wallet
- https://www.bitaddress.org
- http://bitcoin.org/en/protect-your-privacy
- http://fieryspinningsword.com/2013/12/01/how-to-create-a-reasonably-secure-bitcoin-paper-wallet/
- http://bit.ly/JuEe2Q - (כיצד לייצר ארנק נייר - מאת גיל אסייג)
- http://passguardian.com