digital whisper
Technologic Papers

פתרון בעיית התשלומים ב-Bitcoin

מאת יהונתן קלינגר, נדב איבגי וליאור גבעון

מבוא וגילוי נאות

ביטקוין הוא אחד מני כמה מטבעות מבוזרים המופצים באמצעות רשתות עמית לעמית (Peer to Peer) ומבוססים על פרוטוקול של קוד פתוח. בהיבט הפיננסי, ביטקוין מציב אתגרים משמעותיים על הדרך בה אנו תופשים כיום את המוסדות הפיננסיים; אולם, לביטקוין נקשרו מספר עסקאות בעייתיות הקשורות לפעילות פלילית כגון סמים או הלבנת הון, מה שמרחיק ממנו את המוסדות הפיננסיים לאחרונה.

אחת הסיבות שמונעות את אימוץ פרוטוקול הביטקוין בקהילת הגולשים ברשת, מעבר לאוריינות טכנולוגית, היא חוסר הפיכות העסקאות שבו. מצד אחד, מדובר על דרך שבה לא ניתן לעקוץ מוכרים בצורה של הכחשת עסקה. מצד שני, קיומו של מנגנון מסגנון של "הכחשת עסקה" מייצר עלויות עסקה ועמלות אשר מייקרות את מחיר המוצר.

על ידי יצירת מנגנון בוררות, כשם שמוצג על ידי Bitrated באמצעות מערכת ה-MultiSig, ניתן להשיג חסכון בעמלות ועלויות עסקה, ולמצוא מערך שיוכל לטפל בעסקאות Bitcoin אף בצורה שתוכל להכניס ודאות עסקית.

במאמר זה נדבר על היתרונות של מעבר לטכנולוגית MultiSig בכלל, ועל הצורך האבטחתי בכך. לצורך העניין נניח כי אין צורך להציג את ביטקוין כמטבע מבוזר, את היתרונות שלו ואת היקף השימוש בו, ולכן נעסוק בכך בצורה קצרה במיוחד.

לצורך העניין, ובקליפת אגוז, ביטקוין הוא מטבע מבוזר, שאינו תלוי באדם אחד או בבנק אחד, ומבוסס על אמון החברה בכוחו של המטבע. המטבע עצמו אינו הילך חוקי ואינו מוגדר כמטבע, אלא כרכוש לצרכי סחר חליפין. ככזה, ישנם לא מעט גורמים שמקבלים אותו כאמצעי תשלום לגיטימי למדי, כמו שירותי אחסון וכדומה. יש גם חברות המציעות המרה של ביטקוין לדולרים מוחשיים או מטבעות אחרים, ואפילו שמועה על חברות שמציעות כרטיסי אשראי מבוססי ביטקוין. היתרון בביטקוין הוא שהוא לוקח את הטוב משני העולמות: את האנונימיות והשליטה של מזומן, יחד עם המיידיות והאפשרות לקיים עסקאות מרחוק בכרטיסי האשראי.

היתרון המשמעותי של ביטקוין הוא הניתוק שלו מכלכלה אחת מרכזית והפיכתו למטבע של הרשת. מאז הקמתו של ביטקוין, אגב, הוקמו עשרות שונות של מטבעות מבוזרים, כשלכל אחד מהם יש יתרונות וחסרונות אחרים, ובאים לטפל בבעיות כאלו או אחרות בפרוטוקול. אולם, נכון להיום באף אחד ממטבעות אלו אין מסחר משמעותי, בניגוד לביטקוין אשר ניתן לרכוש באמצעותו בשלל שירותים אפילו בישראל.

גילוי נאות: מערכת Bitrated מופעלת על ידי נדב איבגי וליאור גבעון, יהונתן קלינגר חבר בועד המייעץ של המיזם ונותן לו ייעוץ משפטי.

בעיית התשלומים

ביטקוין החל עם מאמרו של סטושי נקמוטו (שהוא כנראה שם בדוי) שמדבר על בעיית התשלומים והיכולת לבצע ניהול של ספרי החשבונות בצורה של עמית לעמית (Peer to Peer) כך שבכל רגע נתון כל אחד מכל החברים ברשת יחזיק עותק של יומן העסקאות הכללי. בצורה כזו, אם לאליס יש מטבע דיגיטלי והיא העבירה אותו לבוב, כל ספרי הניהול הדיגיטליים המנוהלים ביחד יכתבו זאת בספר, וכעת כאשר אדם ישאל "מי מחזיק את המטבע" התשובה תהיה "בוב".

בעיה זו, שנפתרה במאמרו של נקמוטו על ידי יצירה של שרשרת בלוקים שמכילים את כלל העסקאות (Blockchain) שזמינה לכל הציבור לצפיה (כאן), מאפשרת עסקאות בלתי הפיכות; מרגע שהעסקה עברה, אין יכולת להחזיר את הכספים. כך, לדוגמא, כאשר ישנו שוד מקוון שמאפשר גניבה של מיליוני דולרים אזי המחזיקים בכספים יכולים לראות את השוד בשידור חי, אך לא לבטל את העסקאות האלו.

בעיה זו, של תשלומים, קיימת גם כאשר משלמים במזומן, אולם מטרת מאמר זה היא לדון בבעיות המשפטיות/טכנולוגיות הקיימות ולהסבירן, כך שיהיה ניתן להבין את מטרת השירות ב-Bitrated ושירותים דומים.

בעיית התשלומים בעולם האמיתי וכרטיסי האשראי

בתחילת הרשת, סוגיית כרטיסי האשראי והשימוש בהם היו מחסום משמעותי מביצוע מסחר אלקטרוני. עד לאמצע שנות התשעים של המאה הקודמת חברות האשראי סרבו כמעט להשתתף במשחק הדיגיטלי בטענה כי עסקאות מקוונות מסוכנות יותר. עסקאות מסוג Chrageback, בהן אדם מתכחש לעסקה שבוצעה, בטענה כי לא הוא ביצע אותה, או כי הוא לא קיבל מוצר, מסוכנות יותר בתחום האינטרנט: כל עוד אין זהות דיגיטלית חזקה, חברות האשראי אינן יכולות להוכיח כי האדם שביצע את העסקה הוא אכן בעל כרטיס האשראי (בהתחשב בקלות בה ניתן להשיג מספרי כרטיסי אשראי). כך, לדוגמא, באתרים למבוגרים יש אחוז רב יותר של הכחשות עסקה, כאשר אנשים טוענים שלא הם היו מי שצרך את השירותים (הרבה פעמים לאחר שמשפחתם נחשפת לאותו החשבון). סוגיית הכחשת העסקה יוצרת מצב

בו בעל עסק צריך להכין מראש עודף שמיועד למקרים כאלו. העודף העסקי מתחשב בכך שחלק משמעותי מעסקאותיו מוכחשות (בין אם מדובר באתרים למבוגרים או בכלל). כאשר, ברוב המקרים מדיניות חברת האשראי היא לזכות את בעל הכרטיס ולהעניש את בית העסק, ובמקרים חריגים לספוג את עלויות העסקה המבוטלת. התוצר המשמעותי במקרה כזה הוא כפול: (1) לקוחות ועסקים טובים משלמים יותר, למרות שהם לא מבצעים הונאה ו-(2) לקוחות אינם מפנימים את הסיכונים, כיוון שהם יודעי שבכל מקרה יזוכו על ידי חברות האשראי ולכן נכנסים לעסקאות מסוכנות יותר.

מודל אמון בביצוע רכישות

חלק מזירות המסחר ברשת, כדוגמאת eBay, הפעילו מערכת של דירוג סוחרים ועסקים. בצורה כזו, צדדים לעסקה יכולים לדעת כמה עסקאות ביצע האדם בעבר, האם קיבל עליהן דירוג חיובי מהצדדים, האם המוצרים שמכר הגיעו בזמן, האם התשלומים שביצע הוכחשו וכדומה. לשיטה זו יתרונות משמעותיים כאשר צדדים רוצים להכנס לעסקה: היא מאפשרת לתגמל עסקים הוגנים אשר יש להם מוניטין לשמר, ומזהירה אנשים לבל ישתמשו במוניטין לרעה, שכן כל ירידה מינורית מ-100% ל-99.8% דירוג חיובי עשויה להשפיע על מכירותיו של העסק. הבעיה העיקרית במערכת מסוג כזה היא שהיא נתונה למניפולציה בקלות יחסית: מצד אחד, ניתן למכור הרבה מאוד מוצרים לחשבונות פיקטיביים בשמך כדי לקבל מוניטין טוב, או אפילו מוצרים מוחשיים בצורה מוזרה מעט, ומצד שני, ניתן למוטט עסק על ידי כתיבת ביקורות שליליות למרות שלא מגיעות לו כאלו על ידי מתחרים. לכן, האמון אמנם עוזר, אך אינו הדרך היחידה והמובטחת.

מעשי עוקץ והונאה של רוכשים

ביטקוין, בניגוד לכרטיסי אשראי ומערכות אחרות, מכיל עסקאות שאינן הפיכות. המשמעות היא שרוכש אשר ביצע רכישה אינו יכול לקבל את כספו בחזרה. אם כן, איזה סוג של מעשי עוקץ על ידי רוכשים קיימים? הסוג הראשון של מעשי עוקץ הינו כזה אשר משלם בכספים שלא שלהם. לדוגמא, על ידי פריצה לחשבונות קיימים ושימוש בכספים המצויים שם. במצב כזה, כאשר כתובת התשלום של בית העסק מזוהה, מגיע הנעקץ לבית העסק ומבקש את כספו בחזרה, שכן לא הוא ביצע את העסקה. הבעיה? במקרים רבים פעולה זו מבוצעת לאחר שסחורה כבר נשלחה, או שניתנו שירותים עבור אותו התשלום.

מעשי עוקץ והונאה של מוכרים

מעשה העוקץ השני הוא דווקא על ידי מוכרים או ספקי שירותים. הם מקימים אתר אינטרנט מכירתי, המציע מוצרים בתשלום מיידי בביטקוין. לאחר התשלום, הם מתחייבים למשלוח, אשר לעולם לא יבוצע. שיטה אחרת היא הקמת שירותים פיננסיים מבוססי מטבעות קריפטוגרפיים והעלמות עם הכסף. לדוגמא, בשוד הדוגיקוין האחרון (מטבע וירטואלי אלטרנטיבי שצובר פופולריות), נפרץ אתר אינטרנט שסיפק שירותי ארנק וירטואלי. אולם, יש הטוענים כי בכלל לא מדובר על פריצה, אלא על הונאה של מפעיל השירות.

מודלים מקובלים בעולם

אז לצורך העניין, הנה נסכם כיצד אפשר להתמודד עם בעיות התשלום ואי התשלום, וכיצד הדבר נעשה עד כה. הרשימה, ברור, אינה ממצה, אבל היא מכסה את רוב הפתרונות המקובלים שהגיעו. כאמור, המטרה היא לדבר על עסקאות צרכניות קטנות, ולא על רכישות עסקיות (כגון, נניח, הקניה של מניות בחברה, או רכישת נדל"ן). כאשר, במקרים כאלו יש סיכונים מובנים אשר מטופלים בדרך הכלל על ידי ביטוחים רבים ואחריות אישית על נושאי משרה בעסקה.

כרטיסי אשראי

הכחשת עסקה. בתחום כרטיסי אשראי נפוצה השיטה של "הכחשת עסקה". צורה זו של טיפול בהונאות עובדת כך: מבוצעת העסקה, כסף יוצא מחשבון הבנק של הלקוח, ועובר לעסק. כאשר הלקוח שם לב כי לא הוא ביצע את העסקה, הוא יוצר קשר בצורה אקטיבית עם חברת האשראי, ומעביר הצהרה כי לא ביצע את העסקה. לאחר העברת הטופס, חברת האשראי עורכת בירור ומשיבה לו את הכסף, והרבה פעמים אף מענישה את בית העסק על כך.

זירות אלקטרוניות: בוררות

זירות אלקטרונית, כדוגמאת eBay, מפעילות הליך בוררות חובה על הצדדים לעסקה, בה הזירה האלקטרונית מהווה את הבורר. לכך יש יתרון משמעותי של עלויות; אולם, פעמים רבות הזירה נדרשת להחזיק בעצמה חלק מהכסף ולגבות עמלות עבור השימוש בזירה. בהתחשב בכך שחברות כמו eBay מפעילות שירותים שנועדו להגן על הלקוח במקרים בהם העסק לא מספק לו את הסחורה, ולהשיב את כספו, הן צריכות לגבות עמלות אשר יצדיקו את השבת הכסף (פעמים רבות על חשבונן). כלומר, הזירות הופכות לצד מעורב בעסקה.

עסקאות מזומן: התעלמות

עסקאות מזומן, ככאלו, יוצרות בעיה משמעותית: אם מדובר על עסקת המזומן הקלאסית בה אדם רוכש מוצר בשוק פשפשים, אין לו את היכולת לזהות את המוכר, אין לו ודאות שהמוכר כלל יהיה שם לאחר זמן מסוים לספק אחריות, ואין לו את האפשרות לקבל את כספו בחזרה בשום צורה שהיא ללא רצונו הטוב של המוכר (או בית משפט).

חוק הגנת הצרכן וחוסר הרלוונטיות שלו

חוק הגנת הצרכן הישראלי מקנה לצרכנים ולקוחות הגנה משמעותית על פי החוק: הוא מאפשר ביטול עסקאות מכר מרחוק (עסקאות טלפוניות או אינטרנט), מחייב אחריות לשירותי מסוימים ועוד. אלא, שיש בו בעיה רצינית: החוק חל בישראל, ודורש פניה לבית משפט כאשר מפרים אותו. כאשר עסקה אלקטרונית מבוצעת בין שני קצוות תבל, קשה מאוד לאכוף את החוק על סוחר בסין, ועוד יותר קשה לקבל את הכסף בחזרה כאשר העלות של משלוח כתב התביעה בדואר רשום לסין גבוהה יותר מאשר עלות העסקה.

פרוטוקול MultiSig

למרות שהפרוטוקול עצמו קיים במערכת ביטקוין, מערכת MultiSig לא זכתה להרבה הכרה או לכניסה לתוכנות ארנק רשמיות של ביטקוין בצורה פשוטה ונוחה. פרוטוקול MultiSig מתבסס על העקרון הבא: אם P מתוך N אנשים לעסקה יאשרו אותה, אז הכסף יעבור מגורם א' לגורם ב'. אם לא, אז הכסף ישאר בעסקה. הדבר דומה מאוד לשיטת ה-Secret Sharing בה ניתן לאחסן מידע שיהיה זמין גם רק אם P מתוך N אנשים יהיו חיים. הפרטוקול עצמו מוגדר כעסקה יחסית אקזוטית, שלא נדרשת לכל אדם. אולם, Bitrated מיישמת את שיטת ה-MultiSig לצורך ביצוע עסקאות.

שירותי Escrow ושירותי Trust

עד היום, רוב שירותי התשלום התבססו על מערכות של Escrow (נאמנות). בצורה כזו, הצדדים לעסקה נתנו לצד שלישי (נאמן) להחזיק עבורם את הכסף, וכאשר הם אישרו לנאמן להעביר את כספי העסקה, הוא יעשה זאת. שירותי נאמנות קיימים ברחבי העולם ומטופלים לא אחת על ידי עורכי דין. פעמים רבות מטרת השירותים היא להבטיח קיומו של תנאי (נניח, העברת בעלות על קרקע). היתרון המשמעותי בשירותי נאמנות הם האמון והביטוח של הנאמן. נאמנים בונים את עסקיהם על שמם הטוב ועל יכולתם להחזיק בנאמנות נכסים וכספים, ולכן כל תביעה או טענה כנגדם תפגע קשות באמון זה ובשמם הטוב. לכן, בשים לב לשירותים כאלו, הלקוח אשר מסתמך על נאמן יודע כי ברוב המקרים, הנאמן והמוניטין הרב שיש לו לא יפעלו כנגדו.

החסרונות בשירותי Escrow או Trust

החסרון הראשון בשירותי נאמנות הוא כי הנכס נמצא בבעלות מוחלטת של הנאמן. במצב כזה, פגיעה בנאמנות בסגנון פרשת אתי אלון, בה אדם מדווח ללקוחות כי הוא מחזיק בסכום מסוים, כאשר בפועל הוא לקח את הכספים לעצמו, היא אפשרית בצורה טכנולוגית, הגם שיש לה סנקציות משפטיות. הבעיה השניה היא יצירת אמון של הנאמן; נאמן חדש אשר אין לו מוניטין, לא יוכל לקבל אמון ציבורי אלא על ידי סיכון משמעותי של נכסיו האישיים וכניסה לעסקאות מפוקפקות יותר, אשר נאמנים רגילים לא יקחו. מצב זה מייצר גם עלויות עסקה משמעותיות: הנאמן חייב להחזיק את הנכס בנאמנות, חייב לגבות עליו עמלה, וחייב לבטח את עצמו בגין מעילת פנים או רשלנות כדי להמנע מנזקים.

מערכת Bitrated

מערכת Bitrated ושימוש בפרוטוקול MultiSig מבטלת את הסיכונים הקיימים לנאמן מכמה סיבות. המערכת עובדת כך: אליס ובוב מתקשרים בעסקה; הם קובעים כי צ'ארלי יהיה הבורר בעסקה בכל מקרה של מחלוקת בינהם, ומקבלים את הסכמתו של צ'ארלי. אליס מעבירה כספים לחשבון MultiSig של 2

מתוך 3; וכאשר בוב מספק לה את השירות, שניהם בהסכמה יכולים לשחרר את הכספים לטובת בוב. במקרה בו אליס לא תהיה מוכנה לשחרר את הכספים, הרי שבוב יוכל לפנות לצ'ארלי ולבקש את שחרורם. אז, ורק אז, מעורבותו של צ'ארלי בעניין תפתח. כלומר, לצ'ארלי אין עלויות עסקה עד שנוצר סכסוך בין הצדדים. בהתחשב בכך שברוב המקרים אין סכסוך כזה, הרי שקל יותר לנהל את המערכת.

כעת, אם ישנו סכסוך, צ'ארלי יכול להוות בורר בין הצדדים (ולא נאמן) ולחקור את האמת ואת הנסיבות, לשאול מה הסיבות לאי הרצון ולנסות להביא את הצדדים לידי פתרון מוסכם. אם הוא לא מצליח, אז הוא יכול (בהסכמה של לפחות אחד מהצדדים) להעביר את הכספים לגורם שהוא חושב שזכאי לקבלם.

אם נוצר מצב אחר, בו בין אליס ובוב יש מחלוקת, אך לאחר בירור של צ'ארלי הם מאמינים שהוא לא בורר טוב מספיק, אזי הם אפילו יכולים להעביר את הכסף לכתובת MultiSig אחרת, אשר תנוהל על ידי בורר אחר.

השגת אמון באמצעות קוד פתוח

חלק משמעותי מהדרישה במצב כזה היא שהאמון יהיה לכל חלקי המערכת. אם הכספים מוחזקים על ידי פלטפורמה אשר גם יכולה לגשת לכספים, לדוגמא, אז יש צורך באמון באותה הפלטפורמה. מה המשמעות במצב כזה? במצב כזה, אם ישנה מעילה בפנים (כמו במקרה שנחשד בעניין Dogewallet, נניח), אזי כל מנגנוני האמון נשברים בנקודה אחת. לכן, חשוב במיוחד כי למי שמפעיל את המערכת לא תוכל להיות גישה לכספים, ולא יהיה מסוגל להעלים את הכספים במקרים שבהם ירצה לעשות זאת. לצורך כך, יש צורך במערכת שתחולל לכל משתמש את המפתחות הפרטיים שלו, אך לא תשמור אותם, וגם יש צורך במערכת שתאפשר לכל משתמש לוודא כי לאף גורם אחר אין יכולת להגיע לכספיו. דבר זה יכול להתקיים רק כאשר המערכת כתובה בצורה פתוחה, שבה קוד המקור של המערכת זמין לכל אדם, וכאשר לאותו אדם יש יכולת לוודא (בסופו של דבר) כי המערכת עליה הוא עובד היא המערכת אשר הוא בחן את קוד המקור שלה. כלומר, **על מנת לוודא כי אין הונאה, למשתמש צריכה להיות היכולת לוודא את זהות הקבצים שמטפלים בעסקה, ולוודא שאין גורמים אחרים מעורבים באמצע**.

שמירת מידע בדפדפן בלבד

נושא נוסף שיש לטפל בו הוא העדר שמירה של היסטוריה של עסקאות או מפתחות פרטיים בצד השרת. הסיבה לכך היא ששמירה כזו תתאפיין, בסופו של דבר, בכך שיהיה גורם מרכזי שיוכל לשלוט בכספים (ראה את הסעיף הקודם) או שיוכל לתעד את היסטוריית העסקאות עצמן, ולהשפיע עליהן על ידי שינוי מערך הזיהוי במערכת בעתיד. כלומר, גם אם כרגע המערכת לא שומרת דבר, אין כל הבטחה כי שינוי עתידי במערכת, כאשר חלק מהמידע נשמר בצד השרת, לא יאפשר שינויים כאלו. לכן, התנאי השני ההכרחי לצורך השגת האמון הוא שמירה בצד הדפדפן בלבד.

עסקאות ללא תיווך

תיווך, וזירות לכשעצמן, יוצרות שני אפקטים: הראשון, חיובי במיוחד, הוא קיומה של תחרות ועקב כך השפעה על המחיר לטובת הצרכן על ידי שימוש בשיטות כגון מכירות פומביות או העמדה של מספר מוצרים אחד לצד השני. האפקט השני, והבעייתי יותר, הוא יצירה של עלויות עסקה במקביל: כפי שהסברנו, הזירה האלקטרונית יוצרת עלויות בצורה של עמלות עבור שימוש בה, עמלות עבור תיווך וטיפול במחלוקות, ועמלות עבור הכחשות עסקה לא לגיטימיות. כל זה יחדיו מייקר את ביצוע העסקאות מעבר למחיר הממשי שישנו. כלומר, ניתן עוד להוזיל את המחירים לסוחרים הגונים, אשר אין להם הכחשות רבות, כאשר הם יודעים שאין להם צורך במערכת בוררות ברוב המקרים. לכן, התנאי השלישי הוא שהשימוש במערכת יגרום להורדת מחירים.

מערכת ניקוד

השלב הבא, והדרך לקדם את הנושא היא על ידי יצירה של מערכת ניקוד; כלומר, כל צד במערכת: מוכר, קונה ובורר, יקבל ניקוד על סמך היסטוריית העבודה שלו. הניקוד יאפשר מצד אחד לדעת מיהם הגורמים עם האמון הרב יותר לצורך ביצוע עסקאות, ומצד שני, יאפשר גם לתגמל אנשים אמינים במיוחד, או לגבות פרמיה מאלו שאינם כאלה. יתר על כן, הניקוד יאפשר גם לטפל בסוגיית המחיר שהבורר יגבה (כלומר, שבוררים אמינים יותר יגבו מחיר גבוה יותר עבור שירותיהם) וגם לטפל בסוגיית הקצאת הסיכונים (לדוגמא, מי משלם על הבוררות). מערכת הניקוד תאפשר ביקורות חיוביות ושליליות, וצריכה להיות נלווית לתוך פרוטוקול ה-MultiSig עצמו כדי לטפל בבעיות של החלפת זירות מרובה או יצירה של חשבונות רבים באותה הזירה.

סיכום

השימוש במערכת MultiSig יכול להוזיל את עלויות העסקה של עסקאות אלקטרוניות, הוא יכול לאפשר אמון רב יותר בעסקאות, הוא גם יכול לאפשר קיומן של עסקאות שלא היו יכולות להתקיים בלי מערכת כזו (כגון העברה בטאבו של בתים). המערכת יכולה לחסוך עלויות רבות המשולמות כיום עבור שירותי נאמנות, או עמלות שמשולמות לזירות מסחר. לצורך אימוץ רחב יותר של השיטה, אולם, יש לפתח את התוכנות הרשמיות כך שיכללו את המערכת כברירת מחדל, ולאפשר נגישות רחבה יותר לבוררים.