

# Bitcoin - איך מנהלים מטבע באופן מבוזר?



אבי חטברט, חוקר בתכנית לוחמת סייבר INSS

שהלקוח העביר לו תשלום (אך התשלום לא אושר ברשת), אבל אחר כך לקבל הודעה שהתשלום בוטל מכיוון שהמטבע כבר לא נמצא אצל הלקוח (כלומר הוא הועבר כבר לארנק אחר).

זוהי בדיוק בעיית הניצול הכפול של מטבעות, ורשת ה Bitcoin מספקת הגנה מפני מקרים כאלו. על בעל המסעדה להמתין עד לקבלת אישור שהעברת הכסף נרשמה בספרי העסקאות על ידי מספר מספיק גדול של צמתים ברשת. לאחר שיתקבל אישור כזה, יהיה ללקוח קשה מאוד לשנות את המצב ולגרומ לרשת לחשוב שהמטבע הועבר לארנק אחר. אבל כאן נוצרת בעיה אחרת. לפעמים, על מנת לקבל אישור תשלום במהימנות מספיק גבוהה, בעל העסק יאלץ להמתין דקות ארוכות (לעתים אף 10 דקות). פרק זמן לא סביר לביצוע עסקה. אחת הדרכים להתגבר על הבעיה ולהאיץ את אישור העסקה, היא באמצעות תשלום עמלה גבוהה (העמלות בעסקאות ביטקוין נקבעות על ידי מבצע העסקה ומשולמות לאנשים שמספקים את כוח המחשוב למערכת - ה"כורים"). עמלה כזו תתמרץ את הכורים לעבד בזריזות את העסקה ולהעדיף אותה על פני עסקאות אחרות, שיאלצו לחכות לתורן. נושא העמלות ברשת הביטקוין הוא סבוך ודינמי, ולכן זהו אינו פתרון מלא לבעיית העיכוב באישור העסקאות. על אף האמור, המטבע מתפתח עם הזמן וניתן לצפות לחדשות גם בנושא הזה. למרות שעברו כ-4 שנים מאז הגיח פרוטוקול ה- Bitcoin לעולם, אנו מצויים כרגע בתקופה התחלתית וקריטית בחיי המטבע. מתפתחים סביבו ארנקים אלקטרוניים, אתרי מסחר, חומרה ייחודית לכריית בלוקים לניהול הרשת, ועסקים חדשים מצטרפים כל יום לרשימת המקומות המקבלים תשלום במטבע וירטואלי. למרות שיש עוד סוגיות רבות המהכות לפתרון (אחת מהן הוזכרה כאן), העתיד של Bitcoin נראה מבטיח ומעניין.

"איך הייתה הארוחה שלך?" שאלה המלצרית. "מצוינת, תודה! אפשר לקבל את החשבון?" תוך כמה דקות הגישה לי המלצרית פתקית נייר עם פירוט ההזמנה שלי והתשלום, וריבוע קטן בצד המכיל קוד QR. הפעלתי את המצלמה של הטלפון החכם, סרקתי את הריבוע ועל המסך הופיעו פרטי התשלום שלי יחד עם פרטי הארנק הוירטואלי של המסעדה. אישרתי את העברת הכסף למסעדה מתוך אפליקציית MyWallet המותקנת על המכשיר שלי. תוך פחות משנייה פרטי העסקה שודרו אל אלפי מחשבים בכל רחבי הגלובוס. עברו מספר שניות נוספות והמלצרית קיבלה אישור סופי על התשלום. העסקה בוצעה.

נשמע כמו תרחיש דמיוני? לא אם תשאלו את לקוחות המסעדה MEZE-GRILL במנהטן, או ROOM 77 בברלין. שתי המסעדות האלו, יחד עם מספר הולך וגדל של אחרות, מקבלות תשלום במטבע הוירטואלי Bitcoin. ייתכן ובקרוב נוכל לשלם כך גם בתל אביב. איך מתנהל תהליך העברת תשלומים במטבע מבוזר? כיצד הרשת מגנה על משתמשיה מפני שימוש חוזר (ניצול כפול) באותו מטבע?

זו הבעיה העיקרית שעליה יקום ויפול כל מטבע וירטואלי מבוזר. לו היה הביטקוין מטבע וירטואלי ריכוזי (לא מבוזר), אזי הייתה רשות אחת שמאשרת את כל העסקאות המתבצעות בו והיה בכוחה למנוע הונאות. לו היה זה מטבע ממש (לא וירטואלי), גם אז ניתן היה למנוע תרמית מסוג ניצול כפול (בהנחה שאין לאנשים פריטיים יכולת להדפיס כסף). אם כן, השילוב בין שתי התכונות: וירטואלי ומבוזר הוא זה שמייצר את האתגר הגדול ביותר לביטקוין. הפרוטוקול שהגה סאטושי נאקאמוטו מנסה להתגבר על הבעיה הזו על ידי שימוש בשיטות הצפנה המאפשרות לפזר את הסמכות לקבוע אילו עסקאות הן תקפות בין מספר עצום של מחשבים, כך שהיכולת של לקוח אחד בודד (גם אם הוא בעל עוצמת מחשוב גדולה) לייצר עסקה מזויפת תשאף לאפס.

אם נחזור למסעדה, נשים לב כי בית עסק המוכן לקבל תשלום ב- Bitcoin לוקח על עצמו סיכון מסוים. בניגוד למטבע פיזי, שאותו אי אפשר להעביר לשני אנשים בו-זמנית, מטבע וירטואלי הוא בסך הכל רצף של תווים (כמו קובץ במחשב) ומבחינה טכנית אין מניעה לשלוח את הרצף הזה לשני מחשבים שונים. הסיכון הנובע מכך הוא שלקוח שנתן הוראה להעביר מטבע לארנק של העסק, יכול לתת באותו הזמן הוראה נוספת לתוכנת הארנק שלו להעביר את אותו המטבע ממש לארנק אחר שברשותו. במצב כזה שתי ההוראות ששודרו לרשת ה- Bitcoin מתחרות זו בזו, והאחת מביניהן שתיקלט ותתקבל ביותר צמתים ברשת תיחשב לאמיתית. השנייה תיפסל. מה שמחמיר עוד יותר את הבעיה, היא העובדה שללקוח יש יכולת להשפיע על כך שהוראה אחת תתקבל בסיכוי הרבה יותר גבוה מהשנייה, וזאת על ידי נגנון פעולות פעולה שלא נרחיב עליו כאן. בסופו של תהליך, עלול בעל המסעדה לראות למשך כמה דקות

9 ביולי 2013  
מכון למחקרי ביטחון לאומי,  
רחוב חיים לבנון 40, תל-אביב

**אתגרי הגנת  
המגזר הפיננסי**

לקראת אירוע  
**ועידת הסייבר**  
של ישראל  
2013

**INSS**  
המכון למחקרי ביטחון לאומי  
מסגרת המרכז הלאומי לביטחון מידע  
מסגרת המרכז הלאומי לביטחון מידע

תכנית לוחמת סייבר  
המבנית נחשבת על ידי קרן בלז'קוביץ' לטכנולוגיה

**אנשים  
ומחשבים**