מוסרים ד"ש - על גניבת 26 מליון ש"ח ב-Dash

מאת עו"ד יהונתן קלינגר

כתב האישום הוגש בשבוע שעבר כנגד אפק זרק (כתב האישום, כתבה ב-Ynet) על גניבה של כ-26 מיליון שקלים במטבעות קריפטוגריים מסוג Dash; דאש הוא מטבע חצי-אנונימי. לפי כתב האישום, זרד והקרבן, אלקסיי ארומנקו, היו שותפים לדירה.

לכאורה, ארומנקו השקיע מאז 2013 במטבעות קריפטוגרפיים שונים (לא שהיו כל כך הרבה אז).

מתישהוא לפני פברואר 2019, ארומנקו רכש (או כרה, או יצר) בערך 74,990.74 מטבעות דאש; זה מייצג בערך אחוז אחד מכלל המחזור של דאש (נכון ליום זה).

זרד, לכאורה, גנב את המטבעות האלו וביצע חמש העברות לארנקים שונים (אפשר לראות אחת מהן כאן, אך כמה מהכתובות שצוינו בכתב האישום כלל לא היו תקפות, ייתכן שהיתה שגיאת כתיב). עכשיו, כתב האישום טוען שבחמש העברות זרד ביצע ערבול של המטבעות כדי למנוע זיהוי של המקור שלהם; לפחות במקרה אחד, זה כנראה לא נכון.

איך שאני רואה את זה, שתי הכתובות שאכן הופיעו תקינות בכתב האישום עדיין מחזיקות את ההון הקטן שנשלח אליהן; המצב יכול שיהיה שונה בכתובות האחרות:

א. 30,000 מטבעות Dash, שהועברו לכתובת Dash Address: XmbEiJ18q2ntiqk74fXpUY7m6BmGDrT3NU (להלן: "כתובת א'").

ב. 1,499.96 מטבעות Dash שהועברו אף הם לכתובת א'.

ג. 16,001 מטבעות Dash שהועברו בשתי העברות שונות לכתובת Dash Address: Xxh1ADfhTuikPQYW69LXChbEHyEyGoXwpp (להלן: "כתובת ב'").

ד. 15,000 מטבעות Dash שהועברו לכתובת Dash Address: XcG3dm2sWnkdzDbFgxfa5qw3pjtijmCbVB.

ה. 12,489 מטבעות Dash שהועברו לכתובת Dash Address: XqLEYh2WFAVjvgbLEFdbe5hHhnQYDiDq9g.

293	f8a98b9f9d...:1	1.67280021	XrUmQ6tpW2RyNSifKnKYHtDw1YmDaU8rsk	71:3044...2c01 33:033e...3ce0
294	f92b5a1bfd...:1	1.6889543	XtzH2qiRXy3ws4Cb7EPixfyb6pUgkSccX7	72:3045...5801 33:039f...19a1
295	f975cb093e...:1	1.67293049	XwkxNzmG51h3Wkei2AMtSAVPgfsPn6CDpD	71:3044...f001 33:038c...385f
296	fb159c5bbb...:0	1.67958587	XqkCnVBxetr3KmYVfEr6b1YqjGkJ9PNbDL	72:3045...8901 33:02fe...c130
297	fb78edb5c4...:1	1.68287408	Xeu8gyLwf5i7Y65dSESFgmfWWUtbtcWuhu	71:3044...e801 33:03e7...d5c6
298	fb7f419fac...:1	1.67280107	XyxAcwZXqENXXxC6bkKqdGf7LLEcs2gnb4	71:3044...6001 33:023e...3c40
299	fbec0a2b8c...:1	1.67309307	XpZGXNAThvDyzzaPC8Q9eaVhnnzGxH8waW	72:3045...d501 33:0281...5d1f
300	fcc01d3f9e...:1	1.67304423	XsWaJ975qEkCpLJUPcovn3qw8nouCidpCU	71:3044...6501 33:0272...4959
301	fd68ba448a...:1	1.6802631	XqkCnVBxetr3KmYVfEr6b1YqjGkJ9PNbDL	72:3045...8601 33:02fe...c130
302	fdac71711e...:1	1.6747606	XknQuApwoGq6mSiWwEJoF7hgtLzAzcggaGm	71:3044...1801 33:0351...b97c
303	fe3df1440a...:0	1.67312001	XkyJVUYLSExon2a3PeaBjAVR34w2w25iwc	72:3045...de01 33:02df...f712

היופי במטבעות מבוזרים, כמובן, הוא שניתן לנתח את מאגר העסקאות (הבלוקצ'יין) וללמוד מה התרחש. כאן ניתן לראות שבעסקה עצמה, של 12,489 מטבעות מ-303 כתובות שונות נשלחו. זה נראה מאוד מוזר. אבל, אם ננתח את זה ונבין מהן אותם עסקאות של 1.67 דאש, נבין את העניין לעומק.

מטבע דאש עובד עם "צמתי על" (Master Node); מדובר על מחשב שמריץ את התכנה של דאש יחד עם עותק של כל הבלוקצ'יין שלה, וכן מספר שירותים נוסף. כדי להריץ צומת על כזה, צריך שיהיו לך כ-1,000 מטבעות דאש נעולים על ידי אחת הכתובות שלך, שאומר שהם לא יזוזו מהמקום. במצב כזה, אתה מקבל גמול של כ-1.67 דאש בכל בלוק שאתה עוזר לכרות (בהפשטה).

זה אומר שחלק מהכסף שנגנב, לפחות, לא נוצר על ידי השקעה במטבעות אלא על ידי הרצה של צמתי-על. זה גם אומר שאירומנקו החזיק לפחות 27 צמתים כאלו (מהכתובות שאכן היו תקפות). אני מניח שאם מספר דומה מייצג את צמתי-העל בכתובות האחרות אז הוא הפעיל כ-60 צמתי-על כאלה. כרגע, לדאש יש כ-5,000 צמתים כאלה, ואירומנקו כנראה הפעיל אחוז מהצמתים, ולא רק החזיק כאחוז מכלל המטבעות במחזור (לא מעט לבחור שגר בדירה עם שותף באילת).

מכאן לבעיות האמיתיות של רשויות אכיפת החוק: הבה נניח, לצורך העניין, שאירומנקו היה שחקן לגיטימי ודיווח על כל ההכנסות והרווחים שלו, הגיש את הדיווחים לרשות המס בזמן וחי טוב מהריבית שיצרו

צמתי-העל שלו. עכשיו, בהנחה שזרד היה חכם דיו כדי לבצע את ההעברות לכתובות שלא זמינות מהמחשב שלו, ושלא מכר את המטבעות אלא השתמש בהם גם הוא לצרכי צמתי-על, כיצד היה ניתן לעלות עליו?

השאלה של קלות גניבת 75,000 המטבעות מארנקים שונים שהחזיקו כ-1,000 מטבעות כל אחד, והיכן היו המפתחות ששלטו בהן, נראית יותר מתיאורטית כאן. זו לא עסקה אחת שבוצעה בקליק, אלא דרש תכנון מדוקדק ותכנית ב' למקרה שבו יובטח שלאחר המעצר זרד לא ידרש לחשוף את המפתחות שלו. זו גם הסיבה מדוע בקשת המדינה לחלט את המחשב האישי והטלפון של זרד נראית מעניינת: נכון לעתה אין כל אינדיקציה שאירומנקו יקבל את המטבעות שלו בחזרה.

אם למשטרה היתה שליטה בנכסים, הם היו יכולים להעביר אותם לשליטה של אירומנקו, או ללכוד אותם בעצמם, כדי להבטיח שאם לזרד יש עדיין שליטה מבחוץ על הארנקים (קרוב משפחה, שותף סוד או שותף), המטבעות עדיין יוחזרו לבעלים החוקיים. כרגע, לזרד יש את כח המיקוח: בלי להוכיח שיש לו את המפתחות לארנקים יהיה קשה למדינה להוכיח מעבר לכל ספק סביר שהוא מי שהזיז את המטבעות מהארנק של ארומנקו לארנק אחר, או בכלל שארומנקו היה הבעלים של הארנק הקודם. יהיה למדינה מאוד קשה להוכיח שהוא גנב ולא שאדם אחר פרץ או לקח, או שארומנקו העביר בעצמו לצד שלישי מאובטח.

לזרד קיימת עוד טענת הגנה די מעניינת; הוא יכול לטעון שארומנקו ביצע הונאת מס מתוחכמת. מדוע? אם המטבעות של אירומנקו נגנבו, הוא היה יכול להשתמש בחריג בהוראות מס הכנסה כדי להכיר באבדן הזה כהפסד הון: אבדן המטבעות עקב פריצה מזכה אותך להכיר בכך כהפסד, ועקב כך לשלם פחות מס. זרד יכול לטעון גם שאירומנקו התקשר עמו בהסכם (כשותף) להקים עסק חדש; במצב כזה, יש סיכוי שהמשפט הזה יתנהל ברמת המילה-מול-מילה, ויהיה קשה להוכיח. עוד, בהתחשב בכך שבדאש יש אפשרות לשליחה אנונימית של מטבעות (Private Send, הסבר בפסקה הבאה), אז יהיה קשה לטעון שזרד מצד אחד כל כך מתוחכם, ומצד שני לא השתמש בכלי הזה כדי להעלים את עקבותיו.

מערכת דאש עובדת כך שאפשר להפעיל פרוטוקול שנקרא Private Send בצורה כזו, הרשת בעצם מבצעת את העסקה מספר פעמים ומערבבת אותה ביחד עם עסקאות אחרות. לצורך העניין, אם אליס רוצה להעביר מטבע אחד לבוב, היא יכולה לשלוח לצ'ארלי (המערבל) מטבע; צ'ארלי מקבל עשרים מטבעות מעשרים מקורות שונים, ושולח אותם החוצה לעשרים יעדים שונים. בצורה כזו לא ניתן להצביע על מי היה השולח; יתר על כן, אפשר לערבל את העסקה מספר פעמים ולהשתמש ב"צ'ארלים" שונים, כך שבעצם מקור העסקה יעלם ולא יהיה ניתן לזהות בודאות מי שלח את הכספים.

אנחנו עדיין לא יודעים איך התיק יתפתח, אבל אני מאמין שלזרד יהיו דרכים טובות להלחם באישומים נגדו, ויצור תקדימים מעניינים על איך מגדירים גניבה של מפתחות בדין, ואיך מוכיחים שמטבעות נגנבו כאשר המפתחות עצמם נגנבו.